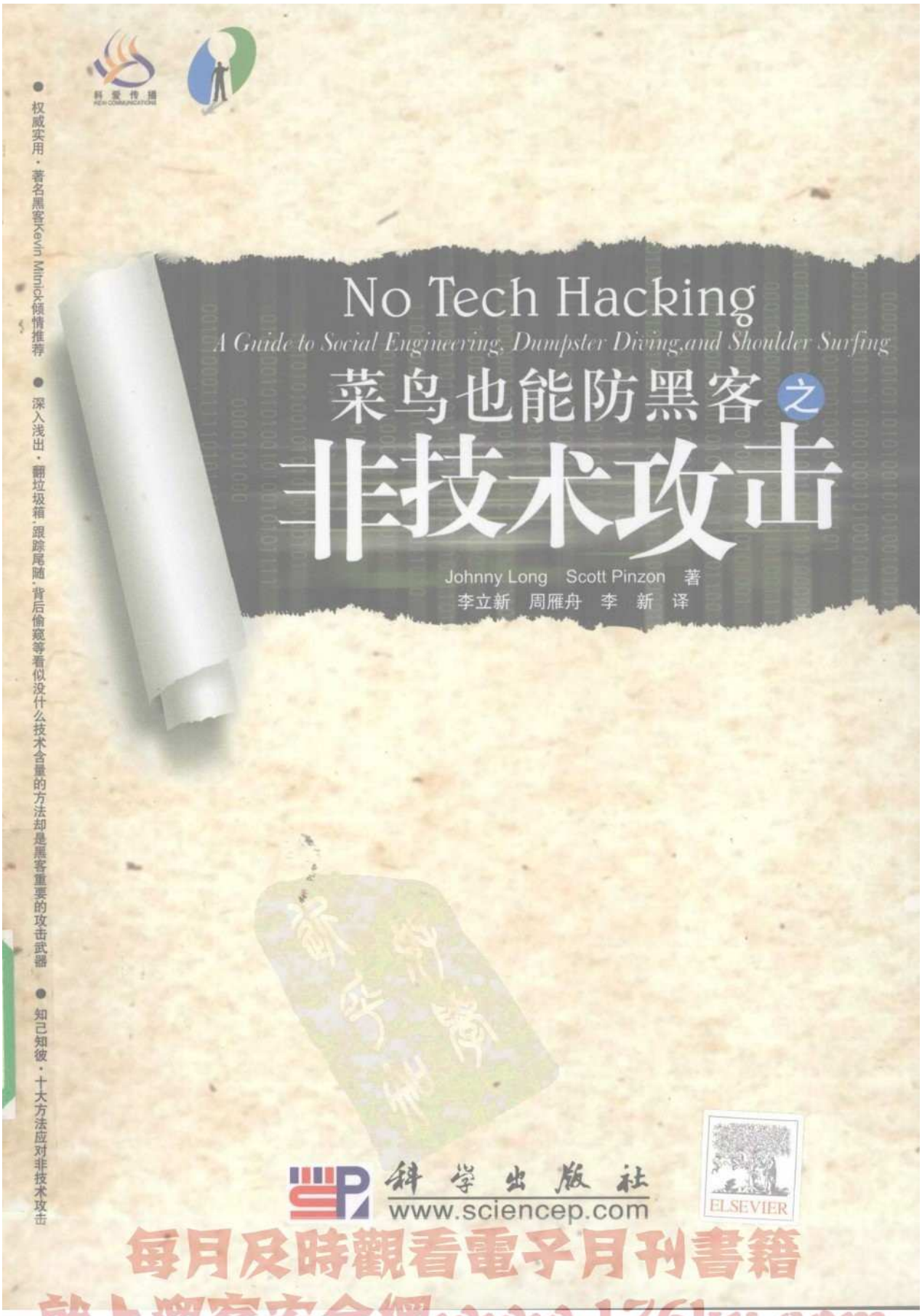


(TP-4362.0101)

SYNGRESS®

ELSEVIER
原版引进

菜鸟也能防黑客之
非技术攻击
No Tech Hacking
A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing

想知道黑客怎样从电脑中获取数据而不留痕迹吗？如何不用碰键盘就能侵入邮件服务器吗？这不是魔幻大片，而是真真正正发生在我们身边。

我们都知道信息的重要性。随着计算机时代的来临，大量的信息以电子的形式存储。而用高科技的电子保护系统来保护信息也就是自然而然的事情。作为一名职业黑客，作者的主要工作就是发现这些系统的弱点。在一次又一次的入侵后，作者发现了可以绕开那些所谓高科技防御系统的方法。本书就是向大家介绍这种方法。正如书名所述，这些方法并不是多么高深的技术，你也一样可以做到。看过本书之后，你会发现在非技术攻击面前，那些所谓的高科技设备是多么的脆弱。

你和你身边的人很可能现在就正在受到此种攻击，你准备好了吗？

科学出版社 科爱传播
http://www.kbooks.cn
editor@kbooks.cn
ISBN 978-7-03-025085-8
9 787030 250858 >
定价：38.00 元

销售分类建议：计算机/信息安全
本版本只限于在中华人民共和国境内销售

No Tech Hacking

A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing

菜鸟也能防黑客

非技术攻击

Johnny Long Scott Pinzon 著

李立新 周雁舟 李 新 译

科学出版社

北京

作者简介

本书的收入将用于 AOET，一个为非洲的艾滋病孤儿提供食物、教育和医疗的组织。它不仅仅是一个援助组织，AOET 的目标是在非洲撒哈拉地区打破贫困和绝望的循环，通过技能培训计划，无论儿童和成年人都能够自食其力，恢复身体健康，重塑对美好未来的希望。通过我在亚马逊网站的关联账号（详见我的个人网站或通过 http://tiniuri.com/f/Xpc）每购买一本书，相应就会为 AOET 捐赠一笔钱，而这些钱足够向一个孩子提供一个月的食物。其他零售（大约占一半的收入）将通过一个联合基金为儿童提供教育、食品和医疗服务。由于我被称为“照顾绝望中的孤儿和寡妇”的人，并且我的个人经验知道这将发挥多么重要的作用。当哈姆雷特感叹：“生存或毁灭，这是个值得考虑的问题！默然忍受命运暴虐的毒箭，或是挺身反抗人世无涯的苦难，通过斗争把它们清扫， 这两种行为，哪一种更高贵？”的时候，他的价值也得到了提升。

我是 Johnny，我是黑客！

此时此刻，我想感谢很多人，而现在又不能当面致谢，但将尽我最大的努力。首先，感谢上帝在我生命中的许多祝福。以基督为榜样，上帝的精神鼓励我以真正的价值观渡过每一天。这本书更多的是上帝的事而非 Johnny 的事。感谢我的妻子和四个孩子。言语无法表达我对你们的爱，感谢你们还我一个真正自己。

我还要感谢 Shmoo 工作组的成员和我的编写团队：Alex, CP, Deviant, Eric, Freshman, Garland, Jack, Joshua, Marc,Ross, Russ, Vince and Yoshi，他们为本书付出了许多心血。感谢你们的支持，特别是在这样紧的时间内。也要感谢 Scott Pinzon，作为一个优秀的编辑和团队成员。您教给了我很多。我也要感谢 Vince Ritts，是您启发了我，在我心中播下非技术攻击的种子。

同时许多朋友和粉丝的支持是我多年工作的动力，再次表示感谢。

请务必访问我们的服务网站http://notechhacking.com，因为我们将继续讲述有关非技术攻击的故事。

Johnny Long 是一个虔诚的基督徒、一个经过培训的职业黑客、一个冷血的海盗、一个训练有素的忍者、一个安全方面的研究员和作家。你能在他的网站 (http://johnny.ihackstuff.com) 找到他。他是 Hackers For Charity (http://ihackcharities.org) 创始人，一个为以慈善为目的的黑客提供工作机会的团体。

技术编辑

Scott Pinzon CISSP 是 LiveSecurity 的主编，一家位于西雅图类似 WatchGuard Technologies 的公司。在其任职期间，他为 LiveSecurity 的 4500 多订阅者编辑、撰写和出版了 1500 个安全警告和最好的解决方法。他已经在安全加密产品、电子商务、语音消息等领域具备了 18 年的经验，由他共同创作和指导的发布在 Google Video 和 YouTube 网站上的 LiveSecurty 培训视频的点击量已经超过了 100 000 次，他也是 *Stealing the Network: How to Own a Shadow* 的编辑。

合 作 者

Jack Wiles 是一个在计算机安全、灾难恢复和物理安全等安全领域有 30 多年经验的安全专家。他还是一个专业的安全培训专家，在一系列有关计算机犯罪有关的主题上对许多联邦机构律师、公司法律顾问代理和内部人员进行了培训。他是一位打上“国土安全”标签的一系列安全领域方面的先驱者。1988 年以来，有 10 000 多人听过他的演讲。他还是 TrainingCo 公司的创办人之一和总裁，并与多家执法机构保持密切接触，尤其是美国的国家安全部门，包括联邦调查局、海关、司法部和国防部，还与其他许多防止高技术犯罪的人员保持密切联系。他还被指定为 North Carolina InfraGard 公司的第一任负责人，该部门已经成为美国最大的公司之一。他也是美国安全服务南卡罗莱纳电子预防犯罪任务组织的创建者之一和核心成员。

Jack 还是一位越战老兵，曾经在 101 空降师于 1967—1968 年在越南服役。他最近刚从陆军退役并保留陆军中校的军衔，在其陆军生涯的最后七年，他被直接指定在五角大楼工作。业余时间，他还是数家杂志的特约编辑。

序 作 者

拥有从事计算机安全行业超过 15 年的经验，Kevin Mitnick 是一个自学成才的专家，发现了复杂操作系统和电信设备的许多弱点。作为一个青年人，他喜欢钻研损害计算机安全的方法、策略、技术，对学习计算机系统和电信系统的工作原理也乐此不疲。

在构建自己的知识体系过程中，Kevin 曾经对某些全球著名公司的计算机系统进行了未经授权的访问，并渗透进入了已经开发的许多更具抗攻击能力的计算机系统。他曾使用了技术和非技术的方法获得了各种操作系统和电信设备的源代码，以研究其脆弱性以及内部工作机理。

作为世界上最著名的黑客，Kevin 成为全球许多报纸和杂志文章中的主题，他作为嘉宾参加了许多的电视和广播节目，对信息安全的相关问题提供专业咨询。除了出现在当地的网络新闻节目中，他还出现在 60 Minutes, The Learning Channel, Tech TV's Screen Savers, Court TV, Good Morning America, CNN's Burden of Proof, Street Sweep, and Talkback Live, National Public Radio 节目中，并且在 ABC 的间谍剧“Alias”中客串演出。他还在许多行业事件中做主题发言，是每周在洛杉矶播送的 KFI AM640 节目的主持人，在参议院作证，为哈佛法学院上课等等。他的第一本畅销书：《欺骗的艺术》（*The Art of Deception*）2002 年由 Wiley and Sons 出版社出版，其第二本书《入侵的艺术》（*The Art of Intrusion*）于 2005 年 2 月出版。

其他作者

Alex Bayly 的生活十分接近普通人，尽管在其妻子的鼓动下，他曾做过一些社会工程学方面的工作。这使得他收集了很多的无用的和无意义的人 ID 卡。目前，作为英国的高级安全顾问，他从事社会工程学和传统的渗透测试。

CP 是 DC949 的一个活跃成员，也是每年公开的网络攻防竞赛 Open CTF 的组织者之一，尽管其正式职业是软件构架师，而他真正的爱好在于信息安全。他开发了一系列的开源安全工具，并在浏览器安全方面继续其研究工作。目前其主要忙于网络攻防竞赛 Open CTF 的扩展和丰富大家的知识。

Matt Fiddler 领导一个财富 100 强公司的威胁管理团队，他对规避锁技术的研究已经导致了数个锁设计缺陷的公开披露。他在海军陆战队时便开始做情报分析员，1992 年加入商业公司。最近，他把主要经历放在 UNIX 和网络工程、安全咨询和入侵分析方面。

Russel Handorf 目前在一家著名的证券交易所做高级安全分析员，也在 FBI Philadelphia InfraGard Chapter 的讨论会上做指导。在此之前，Handorf 为美国联邦政府、州政府、司法部门、相关公司及教育机构做安全顾问，负责培训、安全监察和安全评估等工作。

Ross Kinard 是 Lafayette 高中的学生。他对各种各样的坏点子和物理安全都非常感兴趣，从气筒到撬锁工具等事物都能让乐在其中。

Eric Michaud 是 Argonne 国立实验室脆弱评估小组的电脑和物理安全分析员。他是 The Open Organisation Of Lockpickers (TOOOL) 美国分部的联合创办人，并且积极参与硬件和电脑安全的研究工作。当他不和其他当地或国际的相关组织成员就安全事件进行合作时，可能会在中西部居住。作为一个传统的自学者，他拿到了来自新泽西 Ramapo 学院硕士学位。

Deviant Ollam 是一位网络工程师和安全顾问，最喜爱的工作是教书。作为一个从新泽西技术学院“科学、技术和社会”培训项目毕业的学生，他对研究人类的价值和科技世界的发展之间的相互作用非常入迷。他认为增加安全的最好的

办法是公开漏洞。他曾经在许多大学、会议发表这一见解，其中包括著名的西点军校。

Marc Weber Tobias, Esq. 是一位调查律师和物理安全专家。他曾经写了五本有关刑法、安全、通信的教科书。作为 Organized Crime Unit 的领导者，他曾经为司法部长办公室（Office of Attorney General）、南达科他州政府工作了好几年。Tobias 为许多执法部门做过演讲，同时还与许多国家的顾客和锁具制造商进行了交流。他的公司为特定的政府机构提供内部事件调查服务，也为私人客户提供国内调查服务。Tobias 主要为客户分析高级安全锁和安全系统的性能，并且参加了用来阻止攻击者进入的安全硬件的设计工作。他撰写了著名的《锁、保险柜和安全》（Locks, Safes, and Security），是执法部门必备的参考书。

序

每年我都会参加很多安全会议。我从未错过 Johnny Long 的演讲。Johnny 不仅是安全电路方面最风趣的演讲者之一，而且他的陈述充满了有趣的思想：在降低安全风险的过程中，基础才是最重要的。

Johnny 要求你不仅不能忽略周围最显眼的地方和还要对你周围的环境有更多的了解，他的非技术攻击呈现了一种称为 MacGyver 攻击的技术，这是一种以安全数据为前提的昂贵的安全技术。

企业每天花费上万美金在高技术安全防卫上，却没有关注简单的绕过技术，没有关注非技术黑客正在窃取他们的利益。本书中，Johnny 描写了安全专家应该考虑的可视攻击。在他们匆忙完成任务去解决下一个问题时，许多安全管理人员忽视了简单的缺陷，反而使得他们的复杂的技术形同虚设。

正当安全部门为自己的技术洋洋自得时，却忽视那些简单的威胁，而攻击者正式抓住这点占据了上风。入侵者将会采用攻击最薄弱的环节的方法，而许多看似完美的防护计划却一直在上演《碟中谍》（*Mission Impossible*）中的桥段。Johnny 将会让你很惊讶，他用手巾开锁，跟在一群职员的后面进入了一幢大楼；从垃圾中找出敏感的私人信息；用 Google 和 P2P 网络去挖掘内部职员和顾客之间传递的敏感信息；然后向你显示了所有的这些是怎样向攻击者敞开大门并攻击你的。

商业安全中最主要的因素是人的因素。如果攻击者打个电话给职员就知道防火墙已经关闭，或者能改变设置留一个后门，那么这些昂贵复杂技术将变得一无是处。社会工程学或许是攻击者最喜欢的方法。当你打几个电话就能够从那些没有防备的人那搜集到看上去无害的信息，而这些信息能让你畅通无阻时，为什么还要把时间浪费在某个精细技术的破解上呢？

在过去的生活中，作为一个黑帽黑客，社会工程学能让我创造记录，在几分钟便完成入侵。然后，我必须找到并发现技术的缺陷去达到我的目的。Jack Wiles 在本书中提供的社会工程学例子或许太完美了，显得不真实。不过，那仅仅是借

口——人的想象力可以想很多，很丰富。问题是，你和你的同事、职员，或者你的爸爸妈妈是否喜欢上了它？在《社会工程》这一章将深入介绍非技术攻击通常会运用哪些方法，而我们应该如何防范，并保护自己不受攻击。

本书中，无论普通读者抑或商业用户都将发现有价值的信息，这些信息将引起你的警觉。本书清楚地列举了那些经常忽略的威胁，在设计安全措施保护交易安全时，IT 管理人员应该充分考虑这些威胁。不仅专业读者会发现本书引人入胜，普通读者也将学到关保护自己信息安全的方法和知识，如身份窃取、入室行窃，以及通过电脑加固家庭防御系统等。与其前作 *Google Hacking* 类似，Johnny 再一次向我们呈现了一个有趣但也引人深思的攻击技术。

Kevin Mitnick

前言

什么是“非技术攻击”？

当我进入这个领域时，知道必须站在技术的前沿。我度过了许许多多不眠之夜，顺着我家的网线爬来爬去学习线路。我的实践很有成效，经过几年的努力，创立了一个小但精锐的试验团队。我非常好，很强壮。网络将在我面前倒下。我的同事都尊敬我，我想我是条汉子。然后我遇见了 Vince。

Vince，年纪 40 过半，鹰一般锐利的眼睛，有点像欧洲人，和公司里的那群人混在一起。他经常身着一件黑色皮革外套、一件漂亮的衬衣、黑色的休闲裤，偶尔会戴顶黑色的软呢帽，显得很有气质。他攻击的故事本身就是一个传奇。有人说他曾经是个联邦调查员，为政府的绝密工程工作，也有人说他是唯利是图的天才，把秘密卖给出价最高的人。

他很有才气，能够完成一些看似不可能的事情。他能够用神奇的电子传动装置开启锁，短路电子系统并获取信息。他曾给我展示了一套他创立的系统，叫做“van Eck”[1]。它可以发觉来自 CRT 显示器的电磁辐射，并重新整合，这样就能监视到 1/4 英里远的计算机的显示器。他告诉我一台黑白电视可能用来监听 900MHz 的手机谈话。至今，我仍清楚地记得在地下室用钳子把超高频调谐器和一台老黑白电视连接起来时的情形。当我从旧电视中听到了手机谈话时，就下定决心，要从 Vince 这学到一切能学得东西。

令人难以置信的是，我第一次干这工作是被迫的。幸运的是，我们有不同的任务。我的任务是内部评估，就是评估内部威胁。如果一个职员变成坏人，可能给网络带来无法形容的损害。为了完全评估这些，我们的客户提供工作间、网络接口和一个合法的非管理员用户名和密码。我的任务就是通过这些许可/权限去控

[1] http://en.wikipedia.org/wiki/Van_Eck_phreaking

制关键网络，实现管理。如果我们获得了储存在企业数据库内的秘密记录，我的努力就被认为是成功的。由于我的自信，我有一个接近完美的内部评估记录。

Vince 的任务是物理评估，就是仿效一个外部物理威胁。设备的物理安全特性是顶尖的。他们已经花了很多钱在这些昂贵的锁、传感器，以及监视传动装置上。我知道 Vince 将利用他技术使除去这些东西。我和他里应外合，整个工作就像灌篮一样轻松，我们就是“梦之队”。

当 Vince 让我帮助他评估物理部分时，我大吃一惊。我忽然想起一部 007 的电影，Vince 是“Q”，而我就是 James Bond，去攻击传动设备。Vince 提供装置，像 van Eck 之类的东西，而我渗透进去并暗中监视他们的监视器或其他一些东西。我一想到做这样的事情就想笑，电子键区系统和感应锁都不是我能干的活。当我从监视室的天花板上悄悄取下录像带时，我能想象到守卫的表情。

我迫不及待地想开始。我告诉 Vince 给我那些外国的机械装备，我将用它们去验证安全。当他告诉我没有带任何装置时，我认为他是在开玩笑。当他告诉我真的没有带任何工具时，我差点想把他推倒，但知道他是个黑带高手，因此我有礼貌地问他的想法。他说我们要去创造。真是个小气鬼，什么工具都不提供。我问他不用任何装置如何攻击一个高安全的大楼，他看了我一眼，咧嘴一笑。我决不会忘记那种笑。

我们花了一个早上检查，包括几撞建筑和一些职员停车场，周围都有保护栏。每个人通过前面的大门进出。幸运的是，大门是开的，没有人看守。Vince 开车进去，我们绕过一幢建筑，把车停在它后面，看了看那码头。

“那边”他说。

“哪里？”我问。

“那边”他重复道。

Vince 的幽默感有时很吸引人。当他给我废话时，我决不知道他说什么。我顺着他的手指，看到了一个码头。刚刚通过的大门，有些工人在搬着包裹。“码头？”我问。

“对，就是那里。”

我发出了“哞”的声音。

“正确，简单。”他说。

“我不是简单地说‘哞’，我说‘哞’的意思是那边有那么多人，而你却让我过去。”

“嗯，是的，”他说，“放松一点，就是看上去你好像在这里一样，跟他们问好，友善点，谈论一下天气。”

我照做了。慢慢地，我发现自己就是里面的人了。我在周围转了转，捡到了一些坦克的蓝图，像军用的东西，拷贝了一份，然后离开了。我估计我的心跳达

到了每分钟 400 次，并且开始想像军队监狱是什么样的，不知道关于 Bubba 的谣言是不是真的，但我认为是真的。这是一次难以置信的冲动。这是最简单的社会工程学实践，没一个人怀疑我。我想对他们而言这太尴尬了。当我走进汽车时，忍不住笑了出来。不过，我也没看到 Vince。几分钟后，他从楼里面出来，带着一小堆信纸。

“你是怎么进去的？”我问。

“和你一样。”

“为什么你自己不做呀？”我问。

“因为我开始不确定这样有用。”

我成了 Vince 的小白鼠了。不过没关系，虽然我全身发抖，但准备好了。我们的目标是下一幢楼，看上去像个堡垒。那没有码头，唯一的入口是前面的门。门是木头和钢铁做的（个人感觉很像城堡的门），大约 6 英寸厚，有个读卡器。我看到一个职员刷卡，拉开门正走进去。我建议我们跟着进去。Vince 摇头。显然他有其他计划。他走向大楼，当我们靠近前门时，他慢了下来。距门 6 英尺时，他停下来了。我走了一步超过了他，我回来头来，背对着门。

“天气很好呀，”他越过我看着门说。

“是啊，”我应付道。

“适合攀岩的好天呀。”

我开始转身看那楼。我可不想爬上去。

“别，”他说。“别转身，我们继续聊天。”

“聊天？”我问，“聊什么呀？”

“你看昨晚熊的游戏吗？”他问。我不知道关于他说的什么，也不知道熊是谁，不过他仍在继续说。“老兄，实际上不是那样的。团队的工作方式，它就像……”当前门打开时，Vince 停了下来。一个职员推开门，走向停车场。“他们是单独行动的，”他继续。我受不了了，我转身。门就已经关了。

“废话，”我说“我们可能已经进去了。”

“是啊，一个衣架。”

Vince 有时说些奇怪的东西。但那仅仅是冰山一角。他不是疯子，只是大部分人不能理解而已。我见证了他的狂人时刻。他说：“我们走，我需要一块毛巾。我必须回旅馆。”我不知道他为什么要一块毛巾，但我知道他还是个安全的狂人。我听说过斧头帮，还没听说过毛巾帮。

我们静静地回到旅馆；Vince 看上去仍沉迷在想法中。在旅馆前停下来后，他叫我等几分钟。几分钟后他出现了，拿着一个金属衣架和一块湿毛巾。他把这些东西放在车后面，然后说：“有它们就够了。”我不敢问。他继续说：“用这些东西我们可以进去了。”

我看了他一眼，也不知道我的表情是什么样子，但我觉得应该不会太好。我相信他要么是脑子进水了，要么是鬼上身了。我假装没去听他的，但他继续讲。

“每幢楼都有出口，”他说，“联邦法律规定，在紧急情况下，如果没有人知道出口门的操作方法，出口门必须从里面打开。”我眨了眨眼，通过挡风玻璃看天。我想知道外面的人是否会来接我。“此外，出口不需要钥匙和特别的代号。因此很容易通过出口门离开。”

我问：“我们是不是要对门做些处理。”这话让我十分惊讶。我已经开始跟着Vince 思路往下想了。

他看着我，我知道我看上去是什么样子。我本能地猛击可能在我头上的大蜘蛛。“这就是我们要对门要做的”他说，看着前面的窗口，靠左停下。我们又回到那个地方。他继续说：“那设备的前门很坚固，使用了重型磁性连接系统。我猜它可以抵挡一辆以每小时 40 英里速度行进的汽车的冲击。那些门很厚，可能是隐藏起来的，这系统非常昂贵。”

“但是你有毛巾，”我忍不住说。

“你注意到门上的出口装置没？”

我没有，我不可能说谎，于是承认道：“没有”。

“你必须留意任何东西，”他停下来看着我说，我点了点头。他继续说：“出口装置在一米多高的位置有一个银色的金属门闩。”

我照了下来。“哦，对，推动门闩。”这个词看上去还有点技术含量。

“不，那不是推动门闩。门闩是触摸的，不是压的。当它感觉到触摸时它就会进行操作，非常敏捷。”我们顺利解决了那地方的大门和停车场。Vince 解开扣子，从后座拿了衣架和毛巾。他拆开了衣架，拉成一跟长的直条。叠了一下，把毛巾放在尾端，沿着毛巾折衣架，把整个东西弯成了 90°的白毛巾旗，好像用来向保安投降，我当然不至于问这样愚蠢的问题。“我们走，”他说。

我们走向前门。大约下午 6：00，周围几乎没什么人。他走向那门，从门缝中挤进衣架的毛巾尾端，然后开始扭那衣架。我可以听到门另一边的毛巾的摩擦声。几秒钟后，我听到了一阵低沉的声音，Vince 拉开门，走了进去。我在一旁呆呆地看着，也没注意到门关上了。一会儿门又开了，Vince 伸出头。“你进来吗？”

这可以用以下文字描述：在花费数百万美元去保护他们的大楼后，他们认识到整个系统已经被一条毛巾和一个金属衣架打败了，所有这些都是因为没为门镀上仅仅价值 50 美元的门缝板。主管们表示怀疑，想要证据，这些证据不过是 Vince 走了一圈就得到了。我不知道在向公司演示结果时会发生什么，但是决不会忘记学到的经验：最简单的解决方案就是经常实践。

当然，我们可以破坏大楼的安全系统，先了解锁的磁性操作原理，或者测量墙的厚度，使用的焊条接在天花板上打一个洞，就像电影里一样。但我们不需要

那样。这就是非技术攻击的精髓。你需要掌握大量的技术知识，才能够取得和非技术攻击一样的效果，而这些技术却是没有重复性的。最糟的是，尽管很简单，一个非技术攻击或许是最致命的和最容易误解的。

这些年，我按照 Vince 的建议去学习。我现在注意一切东西，试着保持复杂的思维，几乎从来没有停下过。我经常看到新的攻击手法，而其中最危险的就是有可能被有攻击意愿的人使用的方法。

非技术攻击的关键

非技术攻击的关键就是简化思维、保持清醒、擦亮眼睛、昂起头。例如，当我去商场或其他人口密集的地方时，就会留意周围的人群。对我而言，陌生人是个有趣的难题，我会尽所能去获取有关他们的情况。当我在机场遇到一个商人时，头脑会加速运转，试着辨别他的座位号码和社会地位；了解他的医疗问题；探寻他的家庭情况（或他的性别取向）；推断他的收入水平和经济情况；推测他的饮食习惯；以及猜测他的家庭地址。当我去餐馆时，会观望周围进进出出的人，获取有趣的小道消息。分析周围环境时，我会全心身地沉溺于思考。当我走过停车场时，会留意两边的车辆，推断里面是什么，楼里的居民可能是谁。我做的这些事不是因为注意力集中，而是因为这是我的工作，一种习惯。我已经亲自见证了这种感知的威力。当面对非常棘手的安全挑战时，我不会指责谁。我停下来观察。提高感知能力的最好方法就是时时刻刻都在实战状态。

——Johnny Long

图字：01-2008-5115 号

图书在版编目（CIP）数据

非技术攻击：菜鸟也能防黑客/（美）龙（Long，J.）著；李立新，周雁舟，李新译. —北京：科学出版社，2009

ISBN 978-7-03-025085-8

Ⅰ.非… Ⅱ.①龙…②李…③周…④李… Ⅲ.计算机网络–安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 127815 号

责任编辑：田慎鹏 霍志国 田 伟／责任校对：李奕萱
责任印制：钱玉芬／封面设计：耕者设计工作室

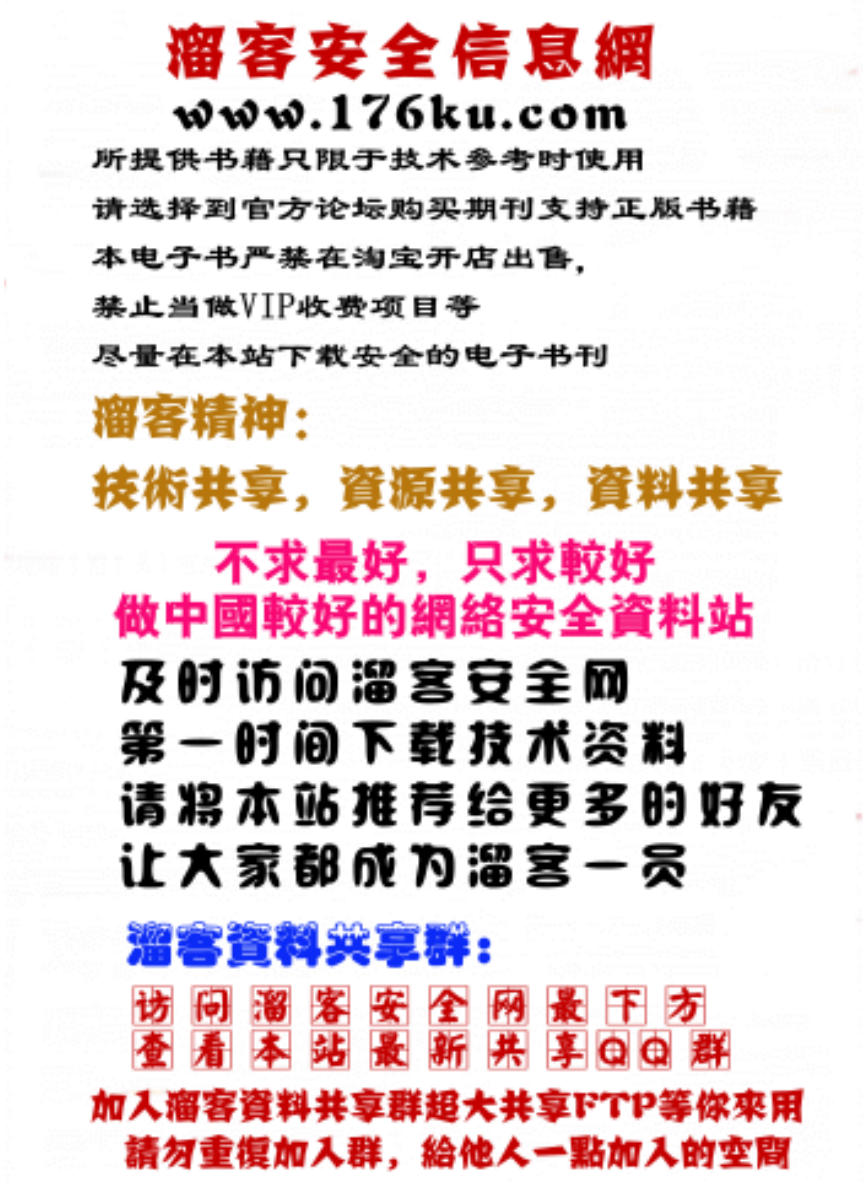
科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

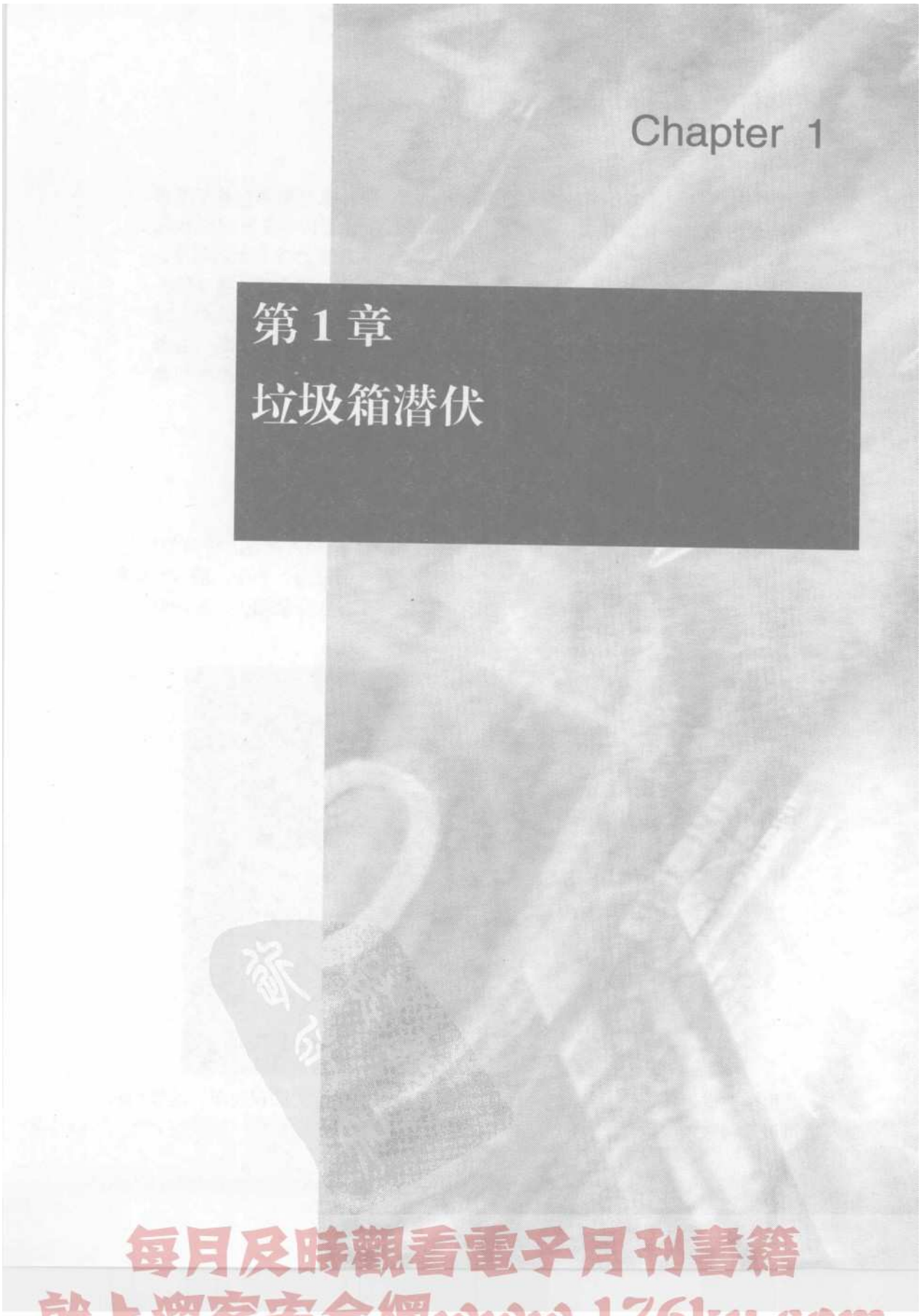
源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销
*
2009 年 7 月第 一 版 开本：B5（720×1000）
2009 年 7 月第一次印刷 印张：15 3/4
印数：1—4 000 字数：373 000

定价：38.00 元
（如有印装质量问题，我社负责调换〈明辉〉）

目录



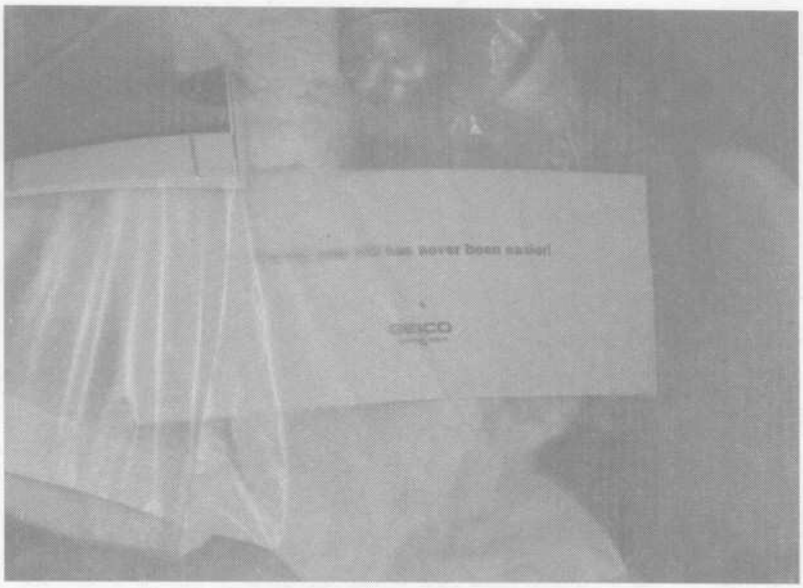


黑客通过许多不同的方式窃取机密数据，但你能想象他们甚至不用接触网络就可以获得某公司的机密数据吗？你可能认为是通过无线网络这种根本不需要接触的技术而实现的，但我要介绍的并非无线网络。看看本章的题目，你可能在想，“垃圾箱潜伏”是什么？是运动项目吗？不是，它是一种方法，黑客通过它不需要任何技术就可以轻易达到入侵的目的。你也许很惊讶，或许会故作镇定，但我劝你最好想想私人数据或公司机密有没有被扔在垃圾箱里，等着某位非高科技黑客把它们拿走？如果没有，那你就不用阅读本章内容了。

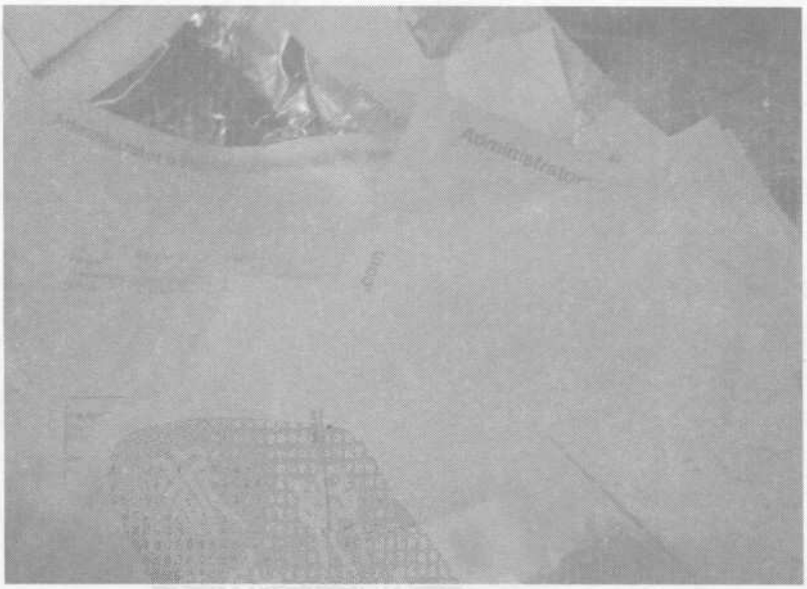
垃圾箱潜伏简介

垃圾箱潜伏（Dumpster Diving）的含义是：潜入垃圾箱内搜寻有价值的信息。我知道这种表达形式不太好，但正是“垃圾箱潜伏”的意思。如今，潜入垃圾箱是容易的。正如下面的照片所示，一些有趣的东西正挂在垃圾箱上，等待有心人拿走。

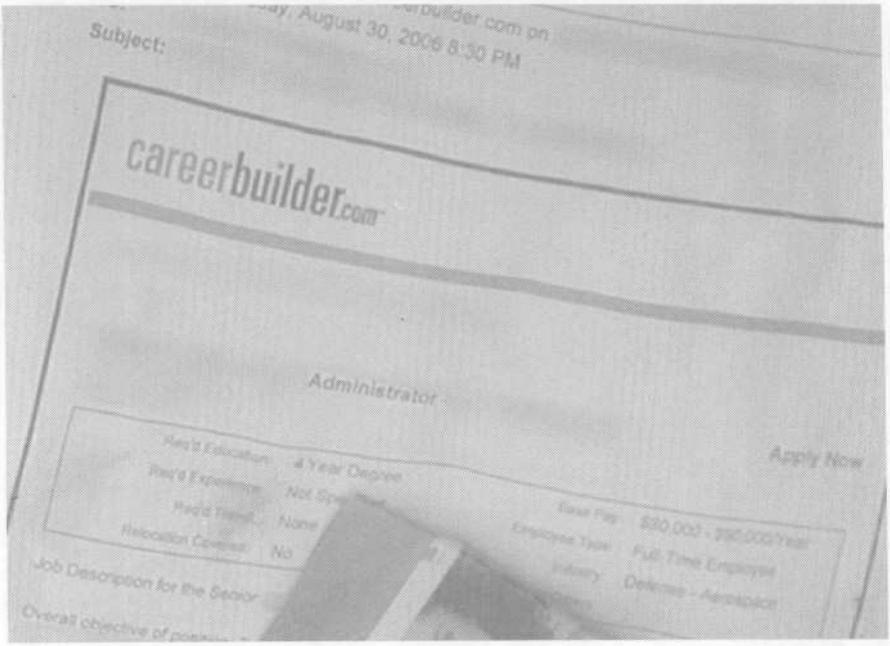
坦率地讲，我总是能找到有价值的垃圾，像下面照片上的保险单，透过塑料袋可以看得很清楚。



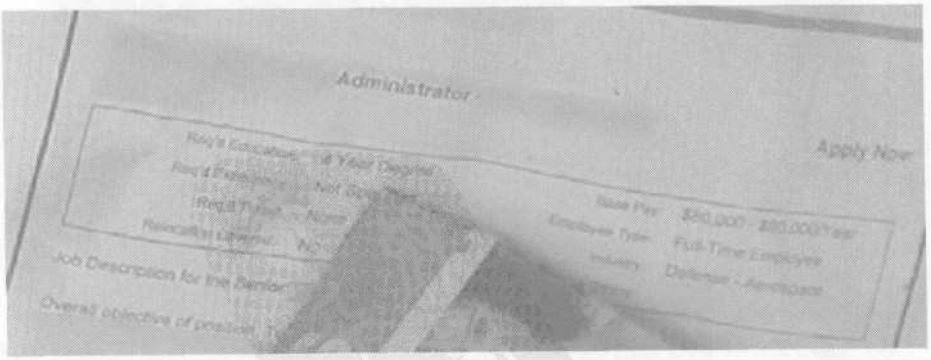
下面照片上是一堆粗心的网络管理员丢弃的文件。直觉告诉我这些文件是一位网络管理员的。



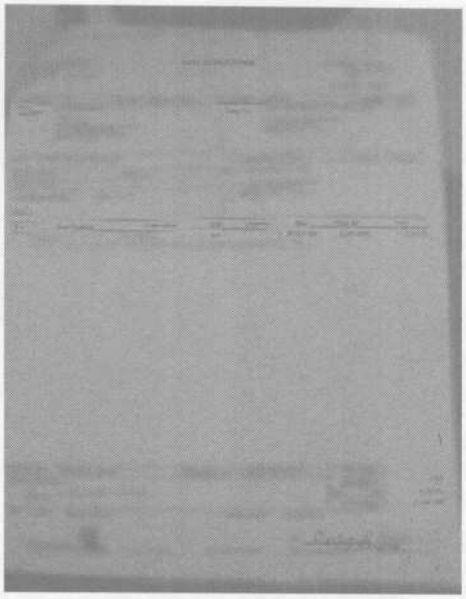
从下面的照片可以看出，Fred 的工作很不顺心，因为他正在求职网站上辛苦地寻求一份新的工作。这份材料揭示了 Fred 许多私人信息。能告诉我还能从中发现其他的信息吗？



首先，Fred 很有可能获得了某种四年制的学位，否则他不会在工作履历中写出这些经历。我打赌他的待遇不错，从工资一栏中可以看到，他年收入近 80 000 美元，他在寻找一份全职工作。还有，他很可能在国防或航空航天部门工作。看到这类文件使我产生了写信给国外情报部门的想法。还可以发现文件中有标记的姓名、邮箱地址、雇主、受教育程度、与国防部的关系，以及职业需求等。通过“翻垃圾箱”这种毫无技术含量的方法，就能获得这些极具价值的资料。

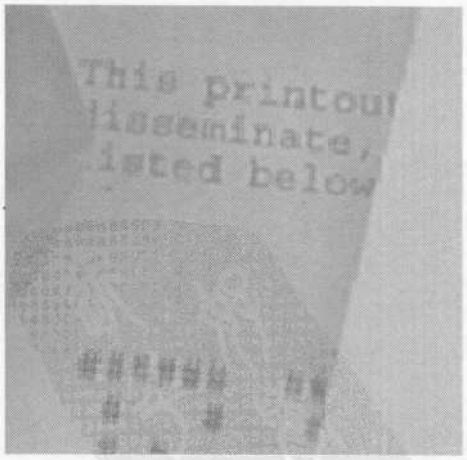


一直以来，我不仅能从垃圾箱里找到一些个人信息，而且能发现一些公司的内部信息。下面的照片是一张购物单，详细记录了某公司的采购情况。

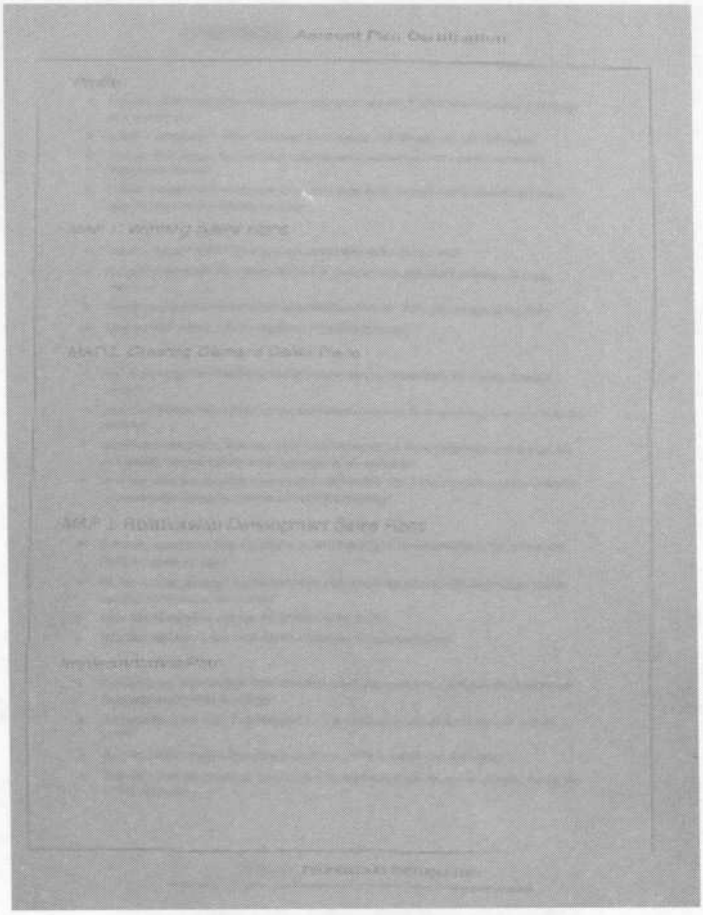


即使表单已经过期，上面仍然有许多重要信息：客户姓名、地址、电话号码、服务描述信息（实际是种相关技术，透露了有关客户服务部门的内部工作机制），以及授权管理部门的签名（如果该管理人还在公司供职，造假者很可能利用这些名字）。

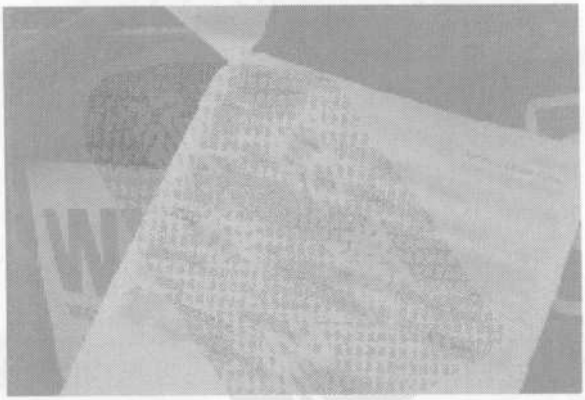
一张购物单的威胁不算大，但下面这个文件可大不相同。上面印有“严禁传播”的字样。



散布这个词太笼统了，我想人们可能不太明白它的含义。但如果把这种文件扔掉了，很显然会产生严重的问题。让人困惑的表达仍然很多，例如“私人信息”。我在垃圾箱旁的捡到的文件上就写着私人信息。如下图。

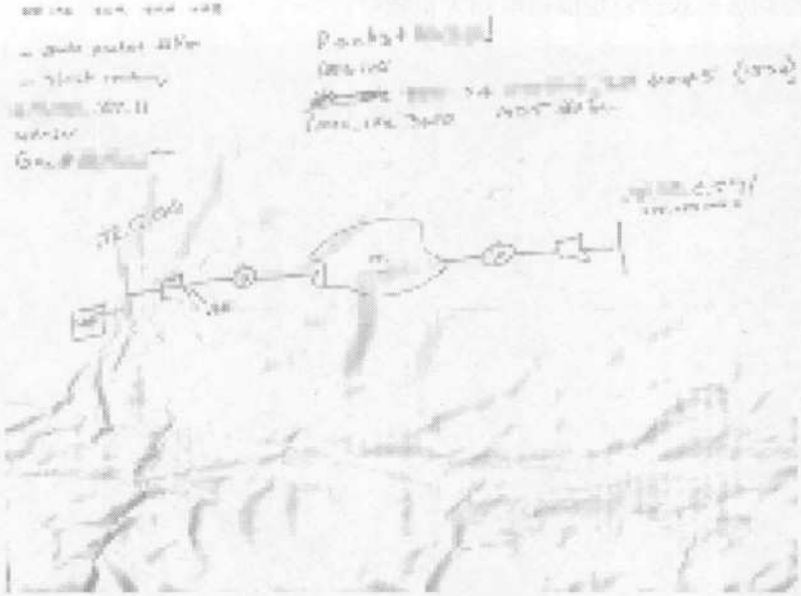


“仅供内部使用”或许是一种较为清晰的表述。但这种表述在一定程度上仍让人困惑，因为我发现在垃圾箱上经常挂着这类文件。



我想我没能理解这类警示短语的含意。正如 Inigo Montoya 在《公主新娘》（一部著名的美国电影，讲述了一对青年男女追求真爱的冒险故事）中所说："你的描述根本没有把真实的意思表达清楚"。我不赞同使用"私人信息"和"禁止散布"这类语句，因为让人搞不清楚这类文件应该怎样处理。我觉得在文件加上标识比较好，例如"将它放在停车场里让大家看"这类语句。当这些文件需要丢弃时，至少不会让人产生疑惑。

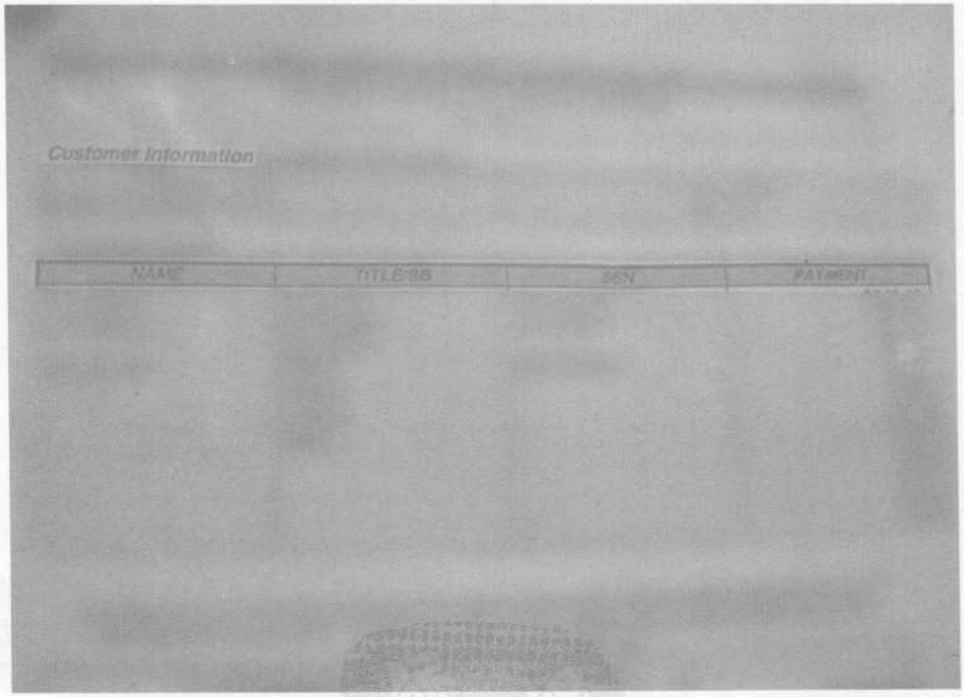
如果你觉得走近垃圾箱很不舒服，不愿去捡挂在上面的东西，我倒有个好主意。有时如果足够幸运，只需在有风的日子里站在停车场里，等着风把秘密文件吹到脸上，而这事的确发生在我的朋友 Mike 身上。他把文件拿下来，发现并不是他老板的，于是他还把文件拿回来让我看。现在我把它拿出来与大家分享。



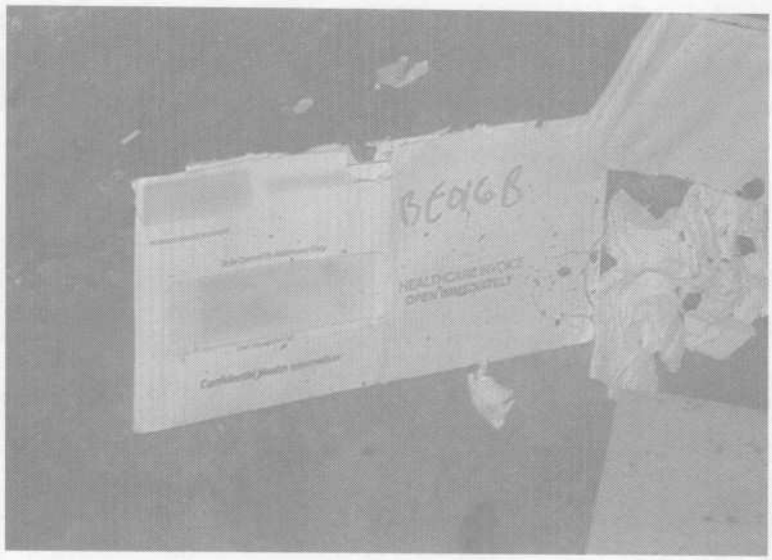
这一连串潦草的字，如果是没经过专门的训练的人，还真不容易认出写得是什么。但任何一名计算机行家都可以告诉你，图上列出了控制某个计算机网络的所有必要信息。其中的 IP 地址是真实的，还有用户名（admin）和密码（看不清了，但是以字母 G 和 a 开头），有了这些信息完全可以管理员的身份登录那台计算机。另外一个写在这张纸顶部的密码（模糊了，但以 R0ck3t 开头），提供了另一个私人计算机的 IP（也模糊了，但以 0.57 结束）或者这个私人网络其他一些计算机的方法。路由器、拓扑图、数据包过滤器、路由配置等专业名词，表明这家伙是个技术老手，另外如 AES128、MD5、ipsec 等专业术语暗示了他（她）至少有安全意识，但这页纸（相关的其他文件 Mike 没有得到）还是被当作废纸扔掉了。

一个技术高超的黑客可能得花几小时、几天，甚至几星期时间去尝试绕过AES128 加密和 ipsec 协议的保护，才能侵入机密网络内部。即使能进入该网络，他（她）还得费大功夫避开内部的安全防护，才能进入核心区域。与此同时，对于一位菜鸟黑客来说，只需站在停车场，等着风吹来的文件就可以在数分钟内轻松绕开整个网络的安全保护系统。

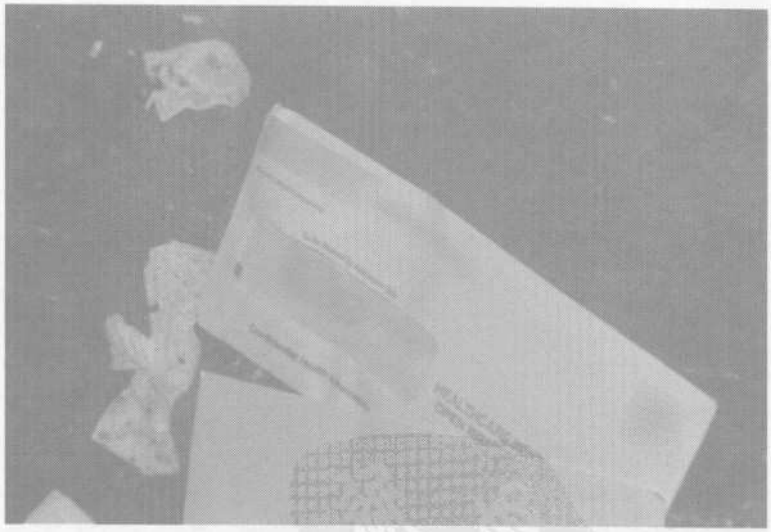
幸运的是，在停车场里碰到这种事情的概率很低。坦白地说，很少能这样轻松地得到那些文件。对于垃圾箱潜伏者来说，大部分情况是这样的，得再走近一点，甚至将头伸进垃圾箱去仔细寻找。在一个打开的盒子上，我找到了一份类似的文件。这份文档中记录着客户的姓名、账户信息，以及推销员花名册，还有他们的佣金和社会保险号码。该公司的竞争对手想必对它们会很感兴趣，而如果某个小偷得到这些数据肯定能窃取到大量钱财。



当我看到下面照片上的垃圾箱时，心里有点失望，显然它刚刚被清空了。只剩一个白信封散落在地上，看起来无关紧要，直到我发现信封上用红色的粗体字写着医疗保健单。下图中信封粗糙、撕裂的边缘似乎表明某个笨蛋急匆匆地撕开信封，拿出发票，然后又把它塞进信封，扔给了像我这样比较敏感的“菜鸟”黑客。如果这是我的发票，我肯定会将撕碎，将纸片放进猫咪的小窝做垫子。这种做法绝对可以对付最出色的垃圾箱潜伏者。



不止一个白信封，我还发现了更多的信封，都写着同样的鲜红色字体。但这些信封（如下面照片上的）都没被打开过，并且信封上的邮寄地址各不相同。



怀着好奇心，我走到大楼前查看了房客的名单。确定无疑，大楼号码簿里有一位医护人员，而我也在捡到的信封上看到了他的名字。那一刻，我意识到扔信封的并非是一个粗心大意的病人，而是一位医护人员。

我隐约记起一些关于处罚医护人员泄露患者信息的事情，好像还有这方面的法律条款。稍后我用 Google（是用 Google，并非 Yahoo）搜了一下，发现《美国国内税收法》（1986 年修正）有关于如何保护患者隐私的规定，即《健康保险责

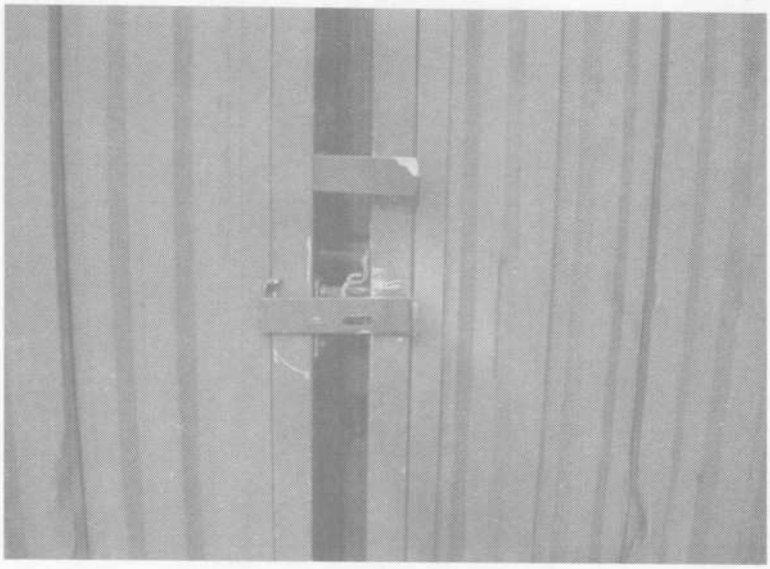
任法案》（Health Insurance Portability & Accountability Act, HIPAA）。法案中特别指出："通过设立强制标准保护患者的隐私和安全"。对恶意违反规定的人处以最高达 250 000 美元的罚款。尽管我知道这样做并非为了那些钱，但觉得如果公司泄密了，相关的人很可能会被炒鱿鱼。

你告诉了他们吗？

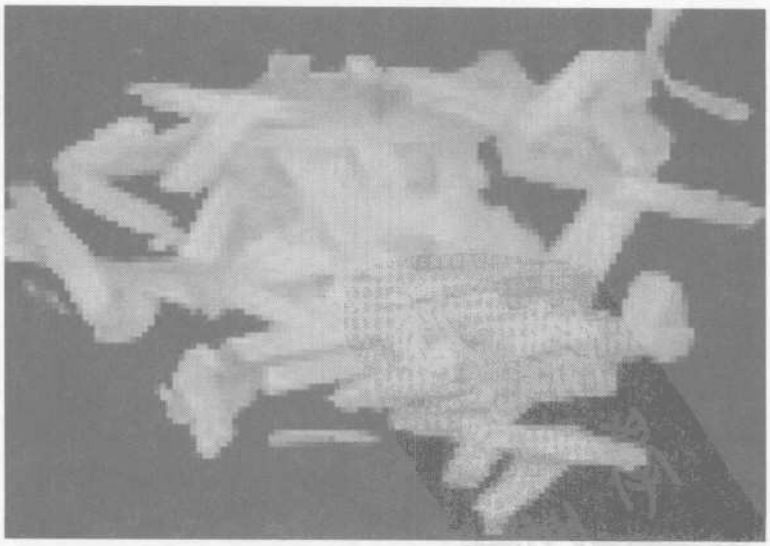
每一章节我都会这样问，它值得重复提问。很多人对这种近似犯罪的行为不留心，我也没主动提醒过他们。从道德的角度讲，我应该提醒他们，但不想这样做。因为很多次我做了认为正确的事情，却被领导训斥，甚至触犯法律。所以，现在我不会再那样做了，而是将这些处理过的照片放进我的书里，以此呼吁大家提高警惕。通过这种方式，这些照片至少能发挥一些积极的作用。

怎样解决这些问题呢？首先，提高对垃圾文件重要性的认识。下面照片上的标识对人们是一个很好的提醒。

锁上垃圾箱的门也是不错的办法。



即使把门锁上，一个有目的的垃圾箱潜伏者可能只需跳过围墙就可以了。使用门锁和垃圾箱锁不失为一个好主意，但当谈及如何处理一些涉密的垃圾文档时，将文件粉碎无疑是条黄金法则。但粉碎只是我个人的观点。市面上有许多类型的碎纸机，碎纸的安全等级也有很多种。一台普通的条带碎纸机将文件沿水平方向切碎。碎片越小，将文件复原的难度越大。例如，一台基本的条带碎纸机将文件切割成 1/8 英寸×1 1/8 英寸的小块。如下图所示。



碎纸机内置一台功能强大的扫描仪，用来监测碎纸片的规格，最终确保碎纸机将把文件粉碎成 1mm×5mm 的粉末状小颗粒，这是最高安全标准。文件经过

这种处理后，即使是世界上最好的特工机构也无法获得其中的信息。

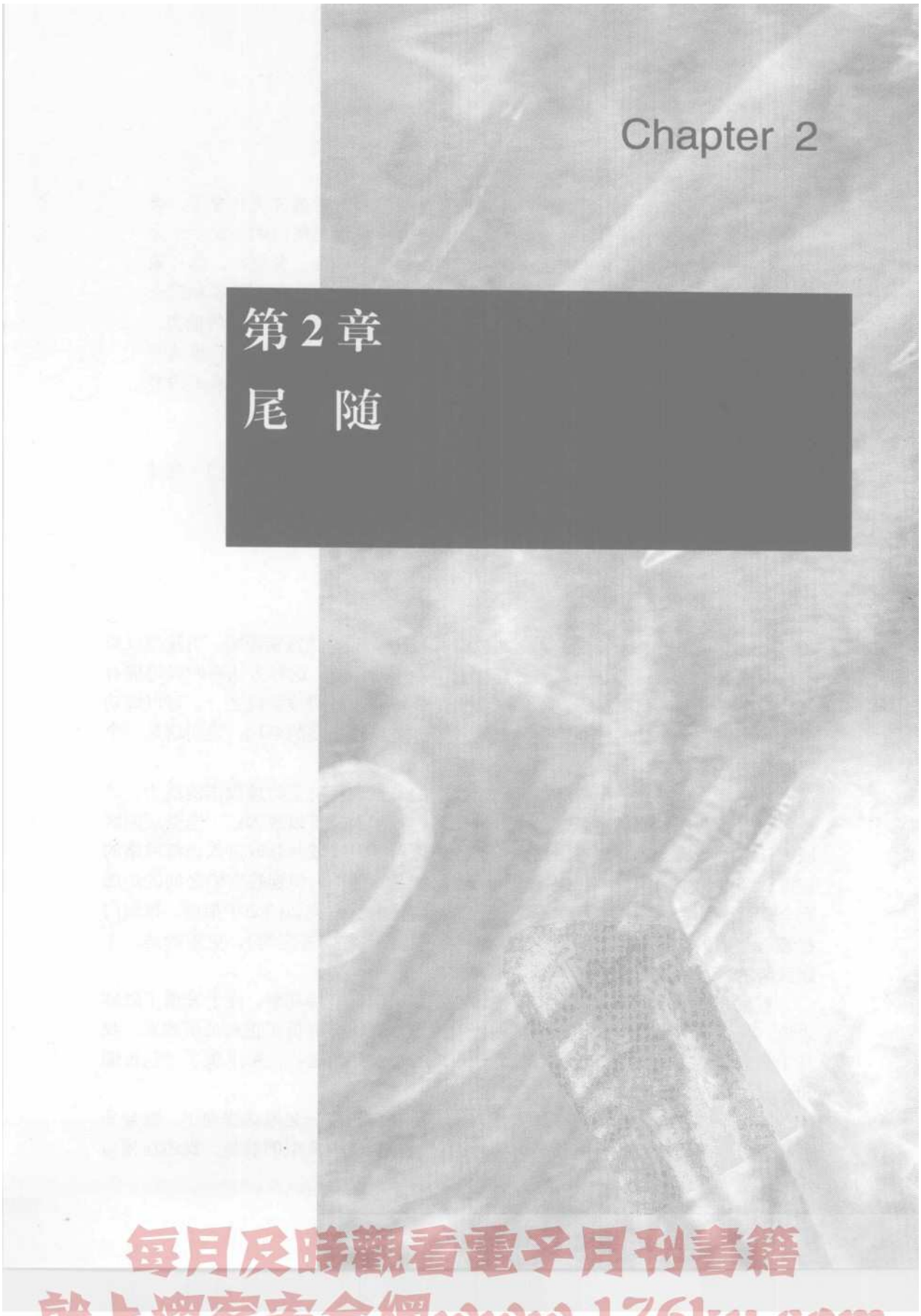
表 1.1 列出了各种碎纸机的具体说明，安全级别从最低到最高。

表 1.1 碎纸机说明

类型	碎片尺寸	目标
竖切	3/8"	普通文件
横切	3/8" × 1 1/2"～3 3/8"	普通文件
竖切	1/4"～1/8"	涉密文件
竖切	1/16"	保密文件
横切	1/8" × 1～1/8"	保密文件
横切	1/16" × 5/8"	机密文件
横切	1/32" × 1/2"	美国国防部和加拿大皇家骑警队认定的高机密文件
横切	1/26" × 1/5" 1 mm × 5 mm	美国政府认定的最高安全级别

一台较好的“微型碎片”碎纸机在商店的售价在 200 美元左右，它能将纸、CD 盘片，甚至信用卡切碎成 3/32×5/16 英寸的碎片，比一般的安全级别要高。通常来说，一分价钱一分货。不管选择什么样的碎纸机，都比将文件直接扔进垃圾箱或停车场好得多。

文件扔掉之前最好确保里面没有重要的信息，以防止落入不怀好意的人手中，造成不必要的损失。如果你是公司安全部门的主管，最好考虑每周检查垃圾桶，看看里面扔的是什么东西，以及它们如何被扔进垃圾箱的。如果想保护自己的隐私，那就买台私人碎纸机，并与家人讨论什么样的东西在扔掉之前需要打碎。如果家人不愿意这样做，应该花时间好好说服他们。要是家人不是特别反对，还可以用另一种方法，就是把垃圾箱的盖子锁上（开玩笑）。



Chapter 2

第2章 尾 随

如果黑客和武士合二为一，那他就是智慧和力量的完美化身了。当然，现实生活中他们也不会合二为一。也许有相当聪明的武士或者十分冷血的黑客。我们来谈谈武士黑客，不过这完全是另一种概念。你可能以为我会从海盗式的武士黑客说起，我们还是先说点别的。黑客和武士都喜欢穿黑色的衣服，并且都有迅速闪入大楼与黑暗融为一体的能力。他们都会障眼法（放出一股烟雾，但有臭味），自己可以毫发无损地穿过墙壁，看起来很酷。你不信？接着往下读，我会一点点揭露真正的非技术黑客（武士）的诡计。

注：如对日本武士如有偏见和误解（与各自文化背景有关），我诚恳地向武神馆的兄弟姐妹们道歉。

引言

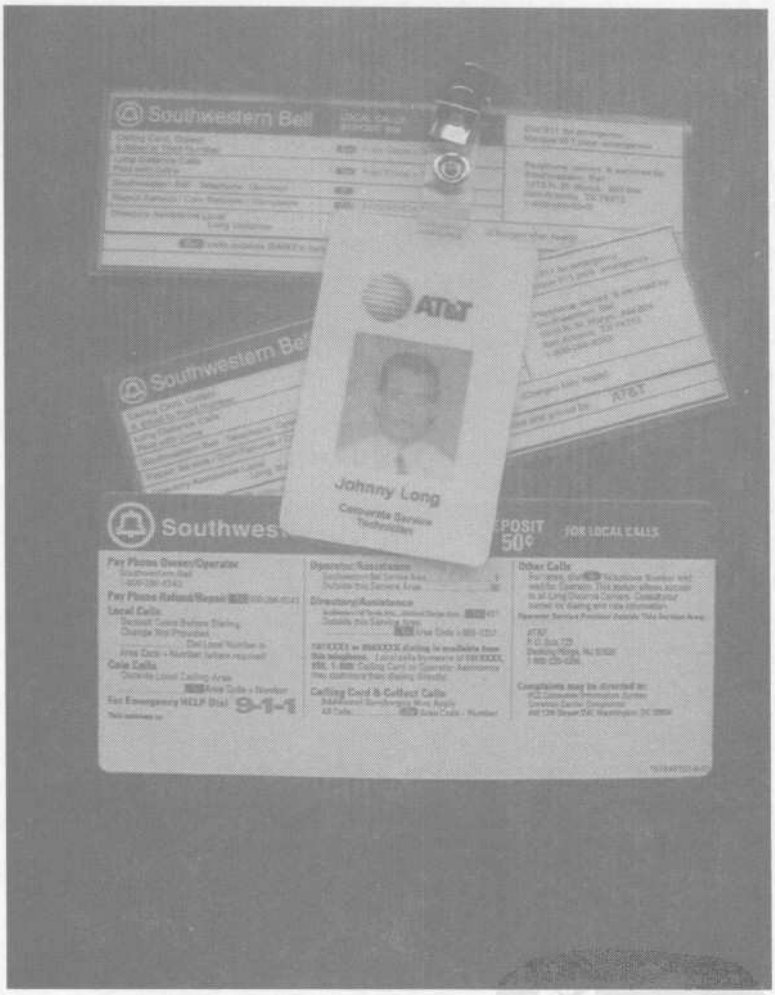
尾随就是跟着某个特定的人走进一幢大楼——基本是紧紧跟随。当我建议跟着前面的人进入目标建筑时，有人建议先用毛巾遮住脸，这种方法有时候可能有效，但往往更容易暴露目标。不过尾随仍是最好的非高科技手段之一，可以成功进入一个有安全防护的建筑。尾随已经成为一个家喻户晓的名词，表明这是一个普遍性的问题。

多年前，我接到一个任务，评估州政府的安全设备防范物理攻击的能力。该设备设置了两个独立的区域，一个开放区域，外部人员可以进入；一个受限的区域，只有内部员工才能进入。我们的任务是进入受限区域并获取进入内部网络的权限。经过初步的探测，我们发现这两个区域是相连的，但连接它们之间的走廊有全副武装的警卫时刻监视。通往保护区域的门前也有类似的防护措施。每扇门都装有坚固的读卡机（没有什么破绽是用毛巾战术可以搞定的）。更糟的是，全副武装的警卫开着警车在停车场巡逻。

看到这么森严的防范，我们有点信心不足，但仍坚持观察，终于发现了破解之道。我们悄悄地躲在通往防护区的侧门周围，发现一群员工正在抽烟聊天。我马上想到了进去的方法。于是，我们朝最近的加油站走去，在那里买了一包香烟和一只打火机。

我准备用社会工程的方法进入大楼。于是我打扮成一名电话修理工。脏兮兮的牛仔裤、工作靴，挂着电话公司标志的白色T恤，很典型的着装。我还在领口

上夹了一个电话公司员工的工作牌。大黄色的工具箱上喷着公司的标志，顶部可以清楚地看到一堆盖章的电话单。工具箱里装满了各种测试工具，再加上一顶破旧的安全帽，活脱脱就是一个电话修理工。



当然，这身像模像样的打扮纯粹是个伪装。电话公司的图标是我从网上下载的；T 恤上的图标是用熨斗烫上去的；衣服领口上的工作牌是我花 2 美元买的。电话单是我从一些当地的付费电话机上撕下来的。不过，电话测试工具是真的，专门为这次行动收集的。至于安全帽，是我在马路边捡到的，破旧的外观反而不会引起别人的怀疑。

靠近这群抽烟的职员不是一个好主意，这和我的演技好坏没有关系。因为如果他们看到我从停车场走来，肯定会认为我不是工作人员。但如果他们走出大楼

的时候我已在那里了，并且烟已经抽了一半，就很可能会认为我是从大楼里走出来放松的。

当他们抽完烟转身往里走之后，我急忙走向侧门并点着一支烟。之后又有两个职员走出来，他们喋喋不休地谈论公司的事务，我也时不时地跟着点头并和他们一起聊。同时我还得确保吐出的烟雾向上扩散，让他们看不出我其实不会抽烟。我发着牢骚，称最近电话老是不正常，他们深有同感地笑笑并和我一起继续抱怨（很幸运），而我一直在担心自己是不是看起来像个新手，尽量不在抽烟上露馅。当他们抽完烟，正了正工作牌准备进去时，我也把烟头弹到马路上（一个烟民的常见动作），去帮他们把门拉开，他们还因此说了句“谢谢”，而实际上正因为他们我才可以进入大楼。进去之后，我马上开始行动。

在大楼里，我畅通无阻地沿着自己的预定路线行进。值得一提的是，我甚至走进了保卫室。值班员惊讶地看着我，直到我指着一张空桌子告诉她那个电话坏了她才开口说话。她并不知道电话是否坏了，但还是让我进来了。毕竟，我是一个电话修理工。我放下工具箱，拿起话筒，听了听拨号的声音。我摇了摇头，将话筒放回托架，从桌上拿起工具箱，顺便带走了一沓看起来很重要的文件。离开保卫室时，我嘴里还在抱怨着报修人员的低级错误，单位老是给我传达错误的信息，这让我看起来像个白痴。那个值班员咯咯地笑着对我说欢迎下次再来。我看出她对我有好感，大概是因为头上安全帽的缘故。

总而言之，今天运气不错。通过一系列简单的、非技术的手段又成功侵入了一个堡垒。从里面带出来的文件足以证明我们曾进入内部，还有笔记本计算机里记录的几百兆字节的机密数据。职员们没有怀疑我，因为他们认出了T恤和证件上的公司图标。既然图标和工具看起来没问题，我就理所当然的成为看起来像的那个人。但我是故意扮成一个技工的，并且来自一个假的电话公司。我选的那个公司确实是一个数据和语音服务提供商，但他们根本不提供本地的硬件维修服务。从外行的角度来看，即使我是该公司的职员，可这里没有我可以做的业务，如果我做了，也不过是测试电话机而已。

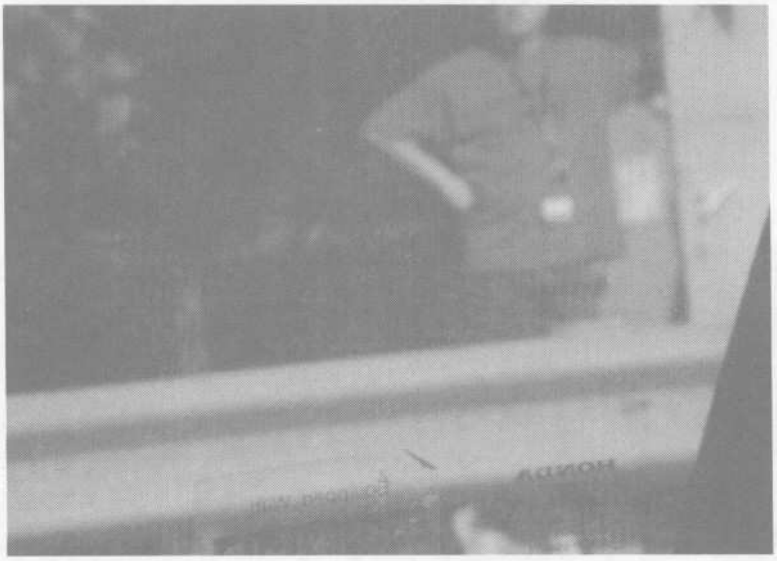
扮演一个可信的角色是成功的关键。我使用原始的尾随技巧获得进入大楼的机会，接着利用一些社交技巧与在楼里遇到的人们闲谈。每位员工只是看到了我的表面情况，根本不会想到我是入侵者，虽然他们中的任何一个都可以阻止这次入侵。

装成电话修理工并不是唯一的方法。根据形势的需要，我可以打扮成邮递员、电工、水管工、电梯维修员，以及任何服务人员。我可以有很多选择。我只需要在适当的时机出现在合适的位置，表现得很有说服力，不让人对自己的角色起疑心。准确地选择地点和时机需要耐心，而与人闲谈需要练习。

打扮成一个角色需要花更多的功夫，但即使如此也不复杂。接下来让我们看如何才能打扮得像模像样，基本要求是什么。

乔装打扮

要有相应的照片做参考。起初，在这件事上我遇到了困难。想想自己依葫芦画瓢的打扮可能让人感觉很别扭，我谨记一定不要在举止上让人看出破绽。开车的时候，我抓拍了一张电话服务技术人员的照片。



看看我车窗玻璃上的标志，可以清楚地看到我当时开了一辆本田。糟糕的是，那家伙看到我在拍他，还一直盯着我开车走过。他或许记住了我的车牌号，并打电话给当地的同事询问。关于这次秘密行动我就说这么多。曾经有一次，我偷偷地拍摄一个邮递员，为得到更好的效果，甚至走出人行道踏进了灌木丛。照片没拍成，却交了个新朋友。那个邮递员小伙很热心地把我从带刺的灌木丛里拉出来。

后来我采用了更为简单的办法就是直接请求我的目标准许我拍几张照片。我很礼貌地提出自己的请求（不要带不敬的口气），大多数人会比较开心地同意。有时候，我会编造一些小故事（如我的小孩喜欢大卡车之类的理由）来要求目标做个动作让我来拍张照片。毕竟，谁会去拒绝一个小孩子请求呢？下面那张照片上的邮递员小伙子非常乐于助人。我拍了他的卡车、全套装备甚至工作牌——足够多的细节来塑造一个可信的邮递员形象。

不要拍摄邮递员

邮递员小伙子让我拍了照片。如果我用他的照片，打扮成他的模样入侵一些地方，他会被解雇或者被处罚吗？基本不会。如果我可以穿成一个邮递员的模样在某栋建筑里走来走去，帮助刺探机密，那它的安全系统就有问题了。事实上大部分人只是凭外表来认识事物。如果一个员工在工作牌上或POLO衫上看到熟悉的标志，会很自然地认为我如表面看起来可信。通常人们在遇到不熟悉的人时会有些尴尬，但如我以前所说的——其实只要保持应有的警惕，我们就不会成功。

不好意思，下图中许多可以辨认的东西我已经做了模糊化处理，但相信我，照片中的人是另一个比较出名的邮递公司的员工。

下图中的技术人员正在利用笔记本记算机努力地工作，他很宽容地允许拍照。虽然他很宽容，但我没有从他后面偷看他的工作内容。

下图中的两位职员中有一个是假冒的，你能告诉我是哪个吗？

下图中的人是一名电气技师还是名黑客？他头上戴着一顶很正式的帽子，并且有电气公司的标志，手里还拿着电子仪器。如果认为电气公司的职员进行野外工作时就是这身打扮，你可能永远不知道其中的差异。

再举最后一个例子，看下图中的技术人员。这种场景在今天的高技术环境中相当常见。显然他在思考一个比较深的技术问题，这个问题可能许多人永远也不能完全明白。在他辛苦工作的时候打扰他有点不太礼貌，所以我只是抓拍了几张照片。

然而，如下图所示，他并非一个普通的技术人员。看出来了吧，他在利用笔记本计算机入侵自动取款机。

这看起来是不是和他之前的样子大不相同？也许不是。他是黑客吗？很有可能。他的奇特装束表明，看起来就是一个自动取款机的维修人员，戴着工作证和所有必要的东西。但是，不是每个自动取款机黑客都带着看似正规的证件吗？

如果心目中的黑客形象是一个有安全意识的公民，则很可能对此严重的误解。想要利用基本的方法接近任何关键技术人员是很愚蠢的，技术人员很讨厌这种事情，而且如果不用他的程序他真的会大发脾气，因为他不停地努力工作，薪水却没多少。换个角度看，如果他有能力入侵一台走廊中的自动取款机，也许就会毫不犹豫地用谎言把你支开。如果他有真本事，会告诉你取下工作证，使他可以尽力维护银行账户的安全，免受黑客利用自动取款机袭击，同时又不与任何人发生冲突。

如何正确地评估环境的安全是件令人头痛的事情，幸运的是，不必担任义务警员的职责。如果你觉得有问题，告诉拿报酬的专业人员。保卫人员、警察、军官、情报机构以及校内巡逻保安都有这些职能，他们都要为辖区内的一切负责。尽管他们除了注意自己的安全外不在乎其他事情，大部分人仍领着工资。所以，如果你告诉他们一个潜在的安全威胁，他们要么做点什么，要么在某个家伙盗窃成功后被炒鱿鱼。无论如何，让他们有个机会干好工作总比当个大厅监视器强。我相信你有比烦扰无知的旁观者更重要的工作要做。

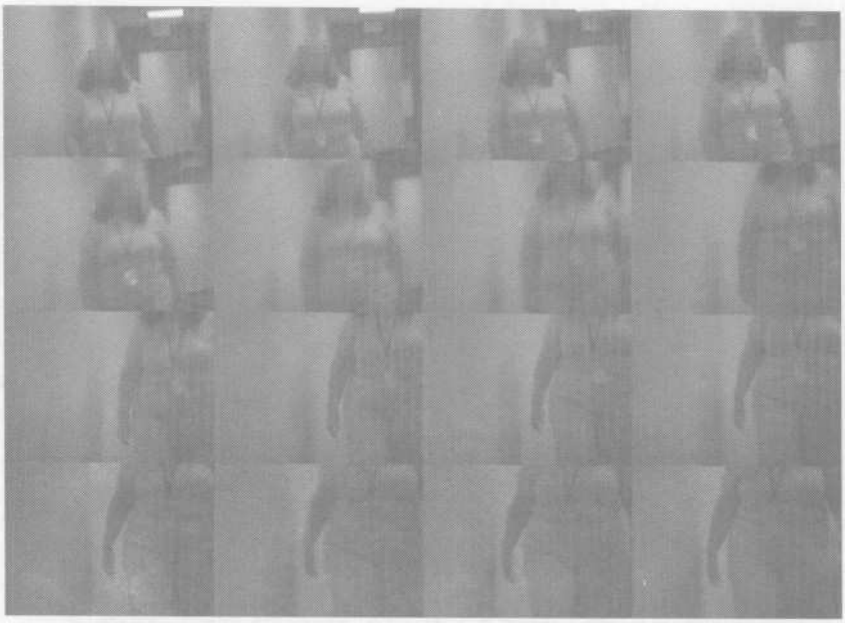
对于管理保卫人员、警察、军官、情报机构和学校内部巡逻人员的人来说，要确保你的人知道如何对付“来客”，并采取正确的措施，而不是做一些毫无意义的事情。注意观察外面有没有发生类似尾随的情况。例如，下图中一位妇女正在走进某政府部门的安全门。

下图是大约 10s 后这扇门的情景。

15s 左右后，门才关上，这段时间对于一个入侵者来说已经足够了，进去的妇女也没有出现。一定要注意这样的情况，一些有企图的家伙肯定会做的。

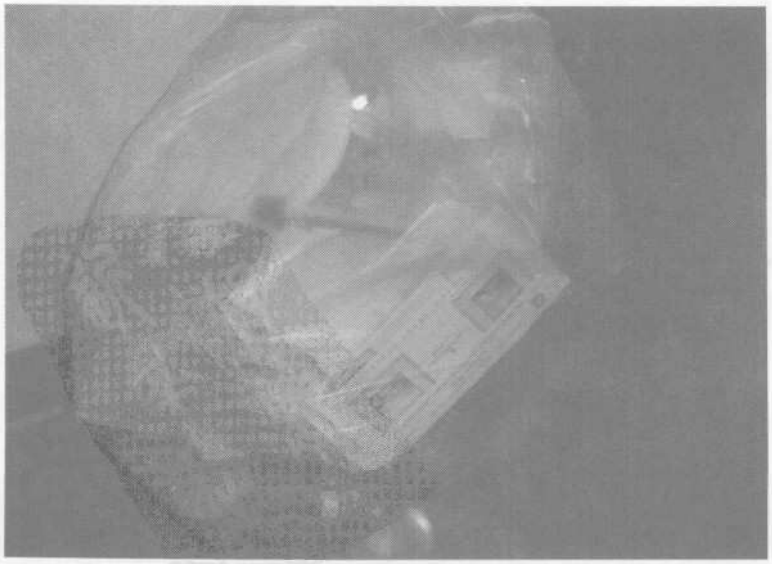
尾随训练

尾随就是跟着一个人进入受保护区域，但进入区域只是开始。下面随我一起体验典型的尾随是什么样子吧。我跟随一个职员通过侧门成功进入了目标建筑。虽然我是跟随在职员后面进来的，但后来发现门根本没锁，上面还有“仅供紧急出口”的标志。一进入大楼，我把照相机拿出来准备拍照。刚准备好就发现过道里走来另一名员工。我迅速把相机放在腰部拍了一组照片，如下图所示。

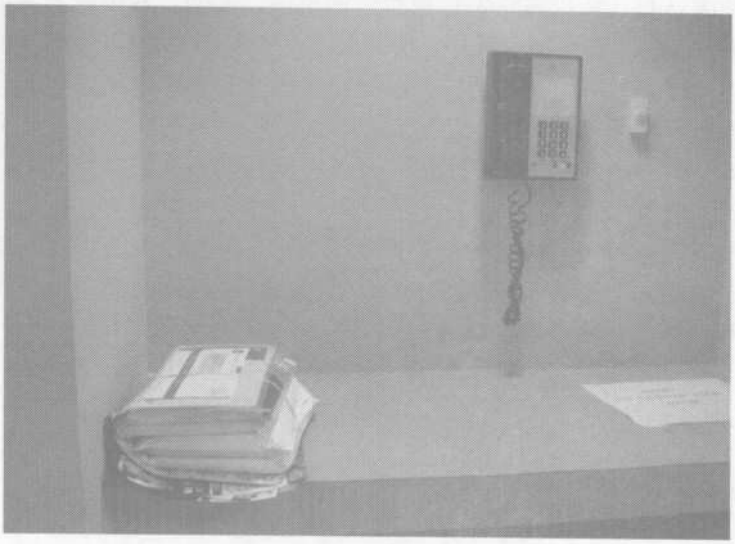


这个夫人笑容可亲且非常友善。这些快照上可以清楚地看到她脖子里的证件和上面的详细信息，但她并非唯一一个没有安全意识的职员。我在大楼里还拍到了其他的职员的证件。

我在楼里还发现了这个垃圾袋，它被扔在一个上锁的办公室的门口。袋子是透明的，可以清楚地看到这是个相当典型的办公室分类垃圾袋：香蕉皮、苏打水罐、纸板和全美速递的票据。

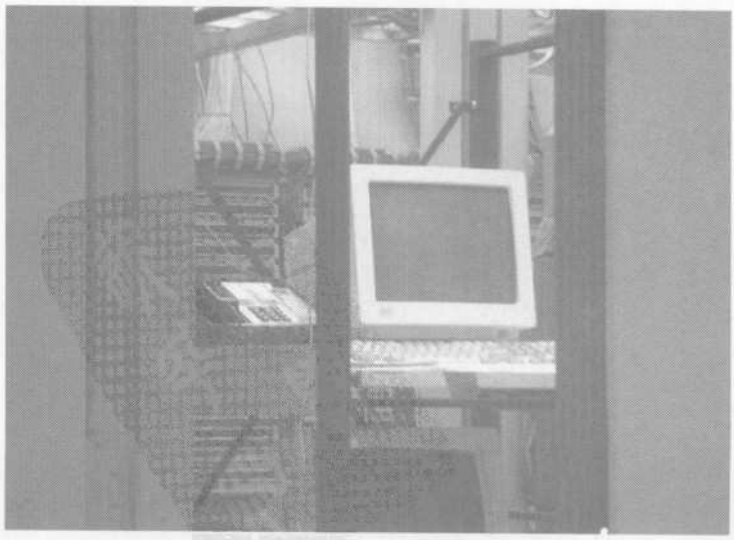


楼里大部分办公室的门都锁着，门上还装有读卡器。既然使用非技术的手段，我便忽略这些地点继续观察别的地方。在一个办公室的外面拍下了这张照片。



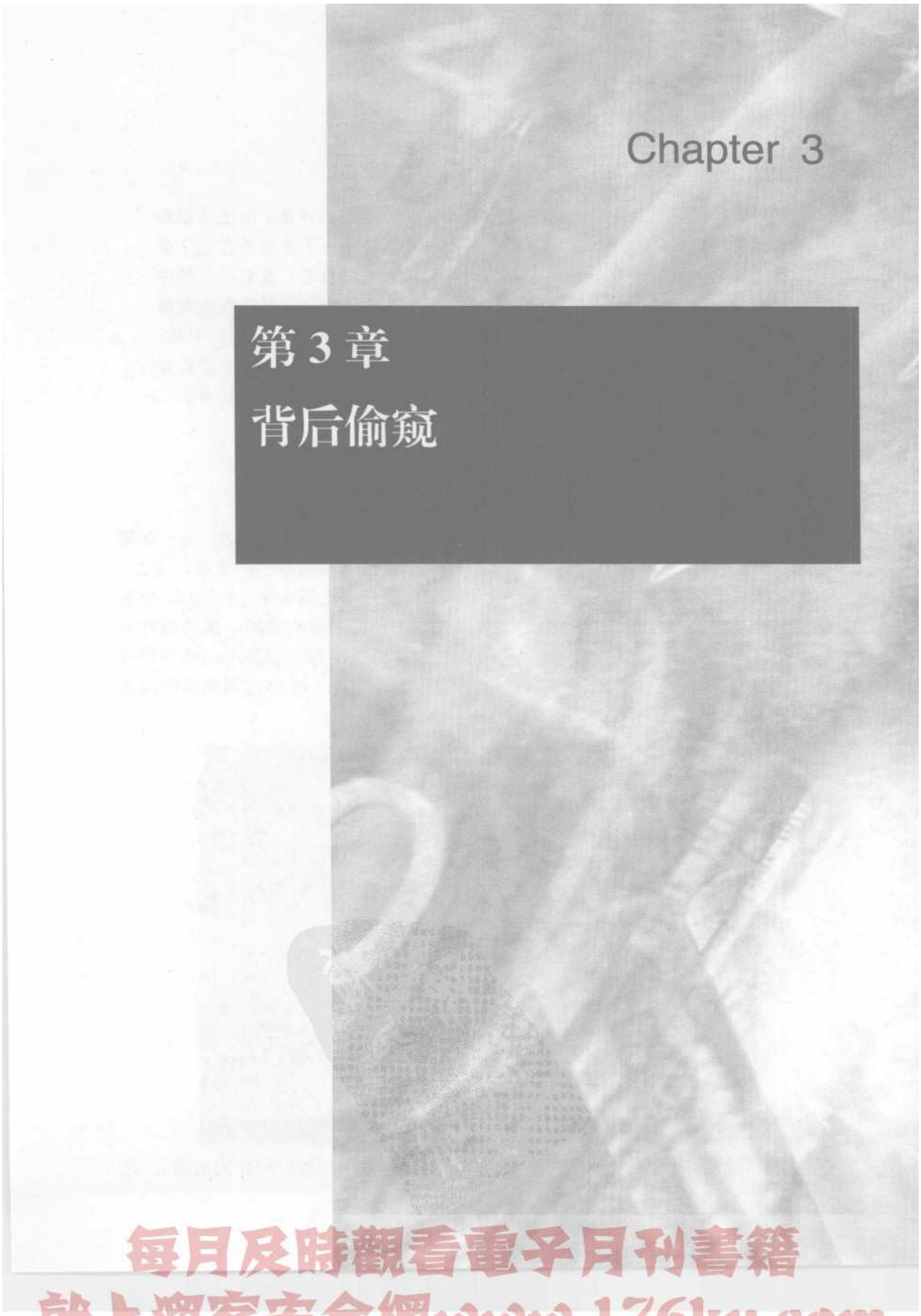
照片里的电话不像以前那样引起我的兴趣。电话上没有通讯簿，而是一些使用说明：呼叫等待、电话会议、呼叫转移、停止呼叫等。不过桌上的一堆邮件引起了我的注意。因为选择了非接触的入侵方式，我就没把它们拿走，但可以看到最上面仍是一张全美速递的单据。

当我继续在过道里走动的时候，看到一个房间的门没有关，从门里看进去好像是个壁橱。我停下来，换个角度仔细观察里面的情况。



原来不是壁橱，而是一个网络机房。这就是尾随者想要到的地方！它就在我面前，大门敞开，基本无人管理。不仅如此，每个控制台程序都已登录，我可以对该公司的电话和计算机网络做任何想做的事情。例如，我可以安置后门程序、放置蠕虫病毒（它能破坏加密程序，嗅探出网络中的加密数据，就像 John Travola 在电影《剑鱼行动》所演绎的那样）以及任何想做的事情。我也可以采用一些在好莱坞电影里不常见到的方法，使用自己编写的程序或密码破解机。无论采用哪种方法，该公司的所有电话、电子邮件及机密信息都在我的掌控下，完全不必使用高技术的手段攻击。

虽然很多设施的安全防护做得都比这个要好，但是在我的职业生涯里所发起的每个现实攻击都要用到一些非技术的黑客手段。生活中注意提高警惕，以黑客的方式思考，你也会发现这些事情。



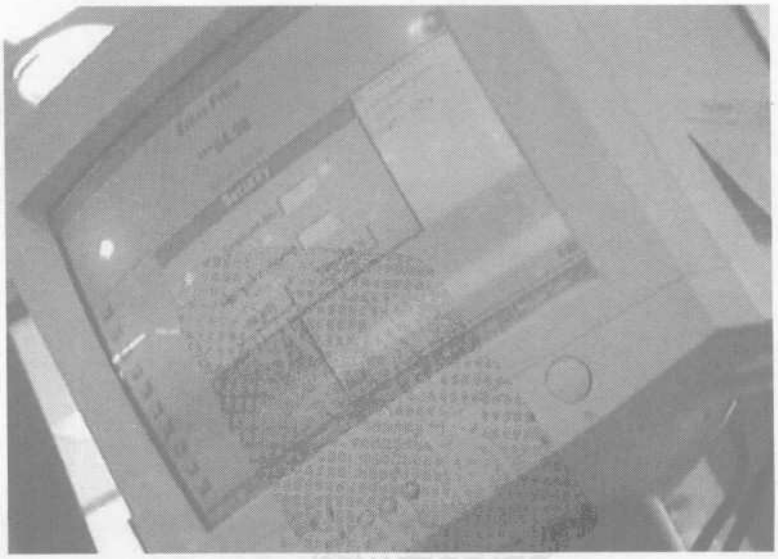
Chapter 3

第3章 背后偷窥

背后偷窥（Shoulder Surfing），直译就是在肩膀上冲浪，听上去很形象，当然这不是一项体育项目，而是一种黑客技术。不要以为自己了解黑客，以为他们会在你输入密码的时候仔细盯着键盘看。我们在电影中经常看到的那些黑客，仅仅动动脑子就可以从笔记本计算机里窃取高级机密。没有可以使用的网络，只有被咖啡因刺激的黑客以及他们的天赋。如果你喜欢盯着笔记本计算机屏幕工作，那可以不用看本章了。假如你看了，明白了背后偷窥的含义，可能马上去掉笔记本计算机显示屏。

什么是背后偷窥

背后偷窥是经典的非技术攻击手段，和肩膀的存在时间一样久远，是一种简单的攻击手段。一个坏小子所做的就是越过受害人的肩膀偷看他的活动。过去，这种方法用来当别人在公用付费电话上输入的时候盗取电话卡账号和密码，然后使用那些信息打免费的长途电话，或者以比市场价低的价格卖掉。虽然现在有许多更简单的方法得到电话卡的相关数据，但是监视键盘在实际中仍然有很多应用。例如，看下面这个装有安全系统的显示屏，它是一个办公用品店的现金出纳机。



和所有的商店里随处可见的终端一样（还有许多用户可以操作的机器），这

台机器需要输入员工的账号和密码。它允许特权操作，前提是输入有效的凭证。经理当然可以拥有比员工和用户（基本不允许）更高的权限。对于一些特定的事务，如高价商品退货就需要经理来登录操作。如下图所示，一位熟练的键盘监视者（或者称为手机偷拍者）能拍下员工敲击键盘时的情景。

一个非技术黑客就可以在客户终端上使用这些信息做任何他们感兴趣的事情。

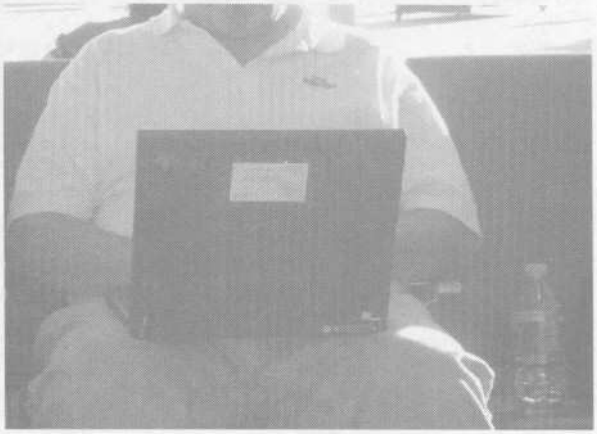
保护自己数据的安全

在公众地点输入密码的时候最应该注意什么呢？输入敏感数据时，在键盘和有企图的眼睛之间制造一些屏障。需要摆正身体，或用另一只手做掩护。如果不愿意这么做，那和不设密码有什么不同？

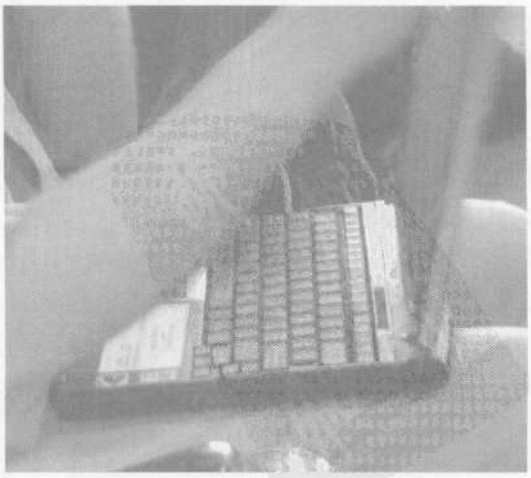
然而，捕捉电话键区的输入数据毕竟有点过时。当世界真正进入数字时代，背后偷窥者会将目光从电话键转移到计算机键盘上，想猎取的不再是电话卡信息而是计算机密码。每当我想要揭穿这种行径时，我脑子里就会浮现《通天神偷》（*Sneakers*）里的经典画面。即使偷拍到数学家输入密码的场景，黑客“梦之队”也会失去耐心，来回倒带，千辛万苦还是不能破解。幸运的是，本章不是关于如何获得瞬间输入的密码，而是让你提高警惕，意识到背后偷窥者已经不仅仅是偷看电话了。

机器外部标签

在介绍实际的背后偷窥技术之前，我们先谈谈如何通过观察机器外部的标签来获取信息。看下面照片中的旅行者。

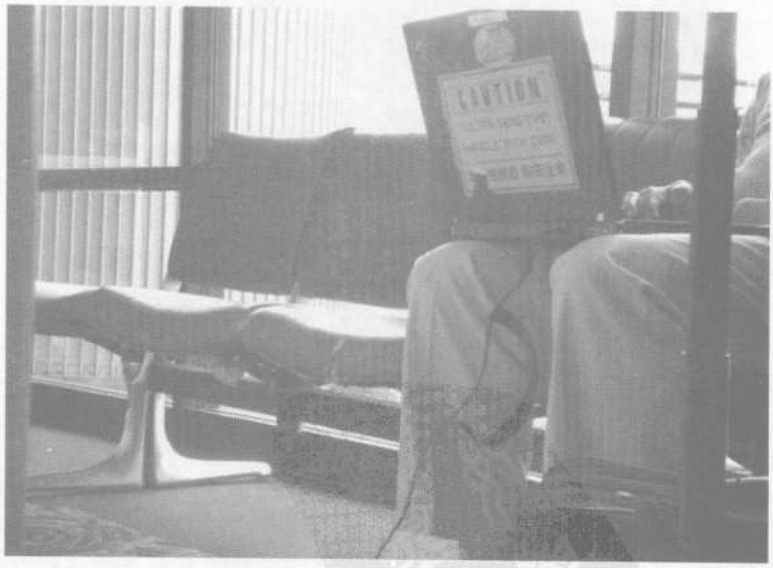


真正的专家很可能已经明白了这台 IBM ThinkPad 笔记本计算机的生产日期、工业模具，因为机器的设计和机身后的接口已经告诉了他。黑客可能在机器后面来回走动，瞥一眼显示屏，尽力去了解目标更多的信息。但一个真正的非技术黑客（或者一位经验丰富的偷窥者）可能会查看贴在笔记本计算机盖子上的商业标签，从中得知目标的姓名、公司、职别、地址，甚至办公室电话和私人手机号码。贴商业标签如今随处可见，俨然成风，下图是我随便抓拍的又一个例子。



用来贴在商品上的卡片是公司提供的关于产品的详细目录。最常见的是一些简单的条形码，也有些比较大，如下图的笔记本计算机上就暴露了相当多的信息。

看下面那张照片，标签贴得真有王者风范。



这台可怜的计算机不仅贴着配置单，还装饰了公司的标志以及超亮的橙色标签，还用中文写着“最高机密”的字样。即使盗窃笔记本计算机的小偷是个文盲，看到这个标签，他也会认为这个笔记本计算机值得偷走。这点很重要。这种标签使得拥有笔记本计算机的人成为小偷行窃或物理攻击的目标。我想起了美国政府

在安全领域使用的一些标签，如“限制”、“机密”、“最高机密”。在政府复杂的工作环境里，我知道这些标签的实际意义，但在政府部门之外也看到了它们的身影。即使是“未分级”的标签，也说明这台设备是在政府部门或相关单位使用的，使该设备成为小偷、间谍或 UFO 阴谋论者攻击的目标。

向标签说“不”

暴露信息的标签不要再使用了。如果不得不在设备上贴，那么在外出的时候，用别的纸条粘在标签上面。这样做至少可以阻止一些过度好奇的眼睛偷看并得到其传递的信息。

在讨论非技术攻击时，如果说到了标签，那就不可能不提到最常见的便签纸。在我的旅程中见到的便签纸不计其数。它们常出现在显示器和桌子上，总会含有一些非技术黑客可以利用的信息。下图是我在一个小旅馆的登记处拍到的，两台机器无人看管。

大家最好不要过分关注塞满每个角落和缝隙以及墙上每寸空间的文件，让我们把目光越过没有上锁的文件柜，来看看计算机和花哨的便签纸。我觉得它们中的大部分没什么用，但有一个看似登录的信息，这说明有台计算机连接到旅馆的网络（从网线看出），也就意味着可以通过这台计算机查询旅客注册信息数据库。一个非技术黑客甚至不用碰任何机器，不做任何违法的事情就可以搜集到相当多的信息。如果有人抓住他呢？他只是一个不太熟悉旅馆的客人，找不到淋浴间的位置而已。

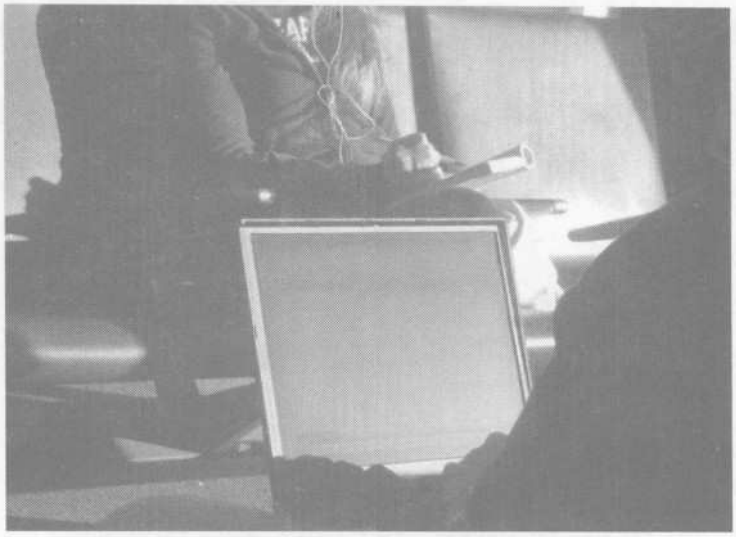
背后偷窥的理想地点

有很多适合进行背后偷窥的地点，但有些地点优于其他地点。先来看机场的情况。

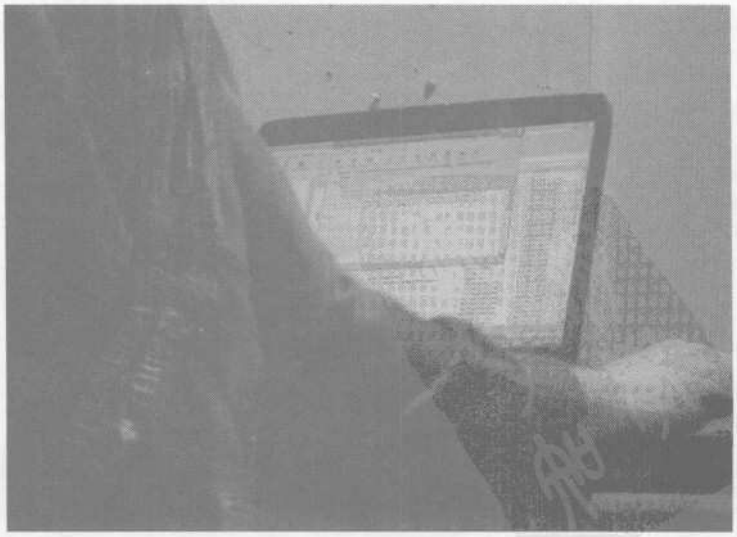
机票检录处，特别是自助服务点有非常好的背后偷窥机会（这点我们将在第9章详细介绍）。在检录过程中，计算机会将旅客的详细信息显示出来，如姓名、目的地、座号、班次。另外安检的时候也是绝佳的机会。

既然逗留在安检处偷拍目标不是明智之举，非技术黑客肯定会去管理员休息室，可以堂堂正正地走进去，然后在里面重操熟练的社交手段。休息室里往往有很多有地位的人在忙自己的事情，而他们大多不会注意背后偷窥者。

大门旁的座椅处也很有趣，由于座椅背靠背的设计，还有疲倦的旅客，他们都很匆忙，注意力比较分散，使背后偷窥者更容易得手。下面的照片就是在这种地方拍到的。

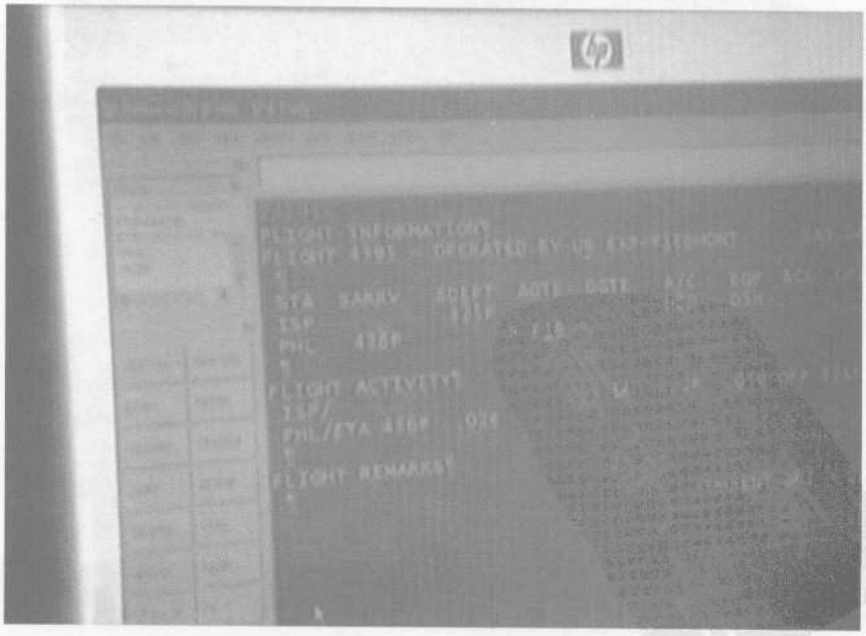


虽然角度不好，光线很糟，但仍能看清计算机屏幕上的内容（为了保护使用者的个人信息，我已经将照片上的屏幕模糊化了）。尽管检录处已经注意保护个人隐私，但是里面充足的光线让偷窥者在相当远的距离处也可以看清楚。下图所示的物品管理处的副主任完全没有注意到我的存在，他此时正忙着发一封机密的内部邮件。

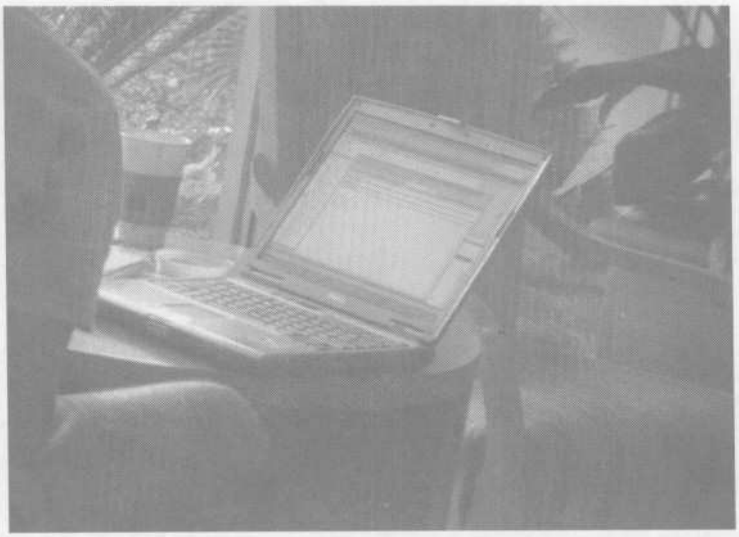


机场内及周围的休息室也有很好的机会偷窥，如下图所示。

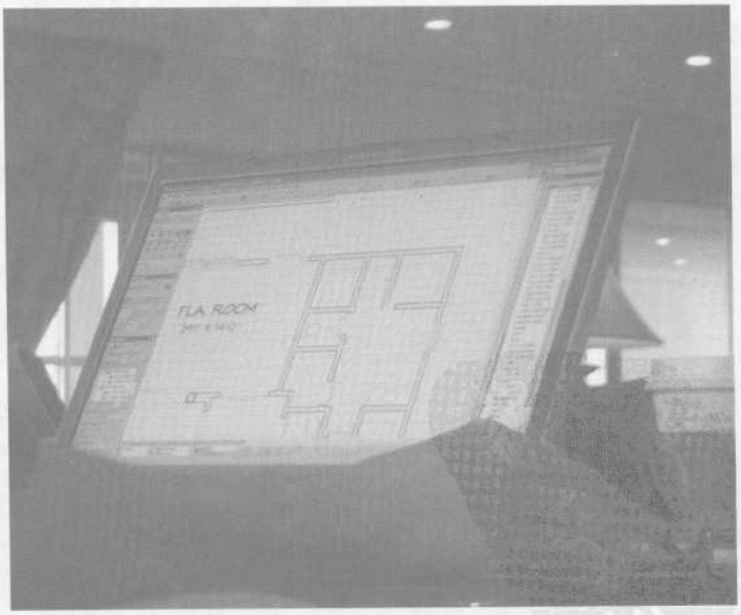
尽管大多数非技术黑客基本不会把机场作为目标，但不会错过无人看管的机场职员工作站。下图中的航班系统在实际应用中的确需要改进。



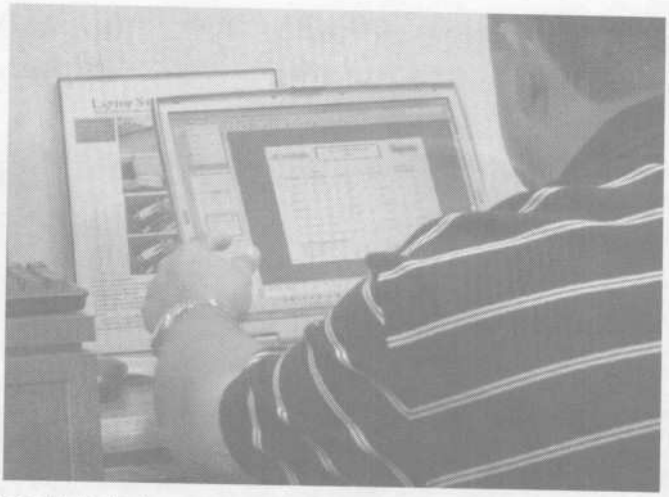
如下图所示，咖啡店也是背后偷窥者比较喜欢的地点。



看起来好像越舒服的地方，人们的警惕性越低。下图中，我就看到了很多东西，从建筑设计图到发给政府部门的机密邮件，内容是一些建议文档，还没有编辑完成。其他的非技术黑客看了照片后告诉我更多有趣的事情。



商业休息室不仅为黑客也为背后偷窥者提供了很好的机会，如下图所示。



在宾馆的商业休息室里工作是否重要呢？相当重要。背后偷窥者很清楚这点，所以要提高警惕。

注意保密、注意安全

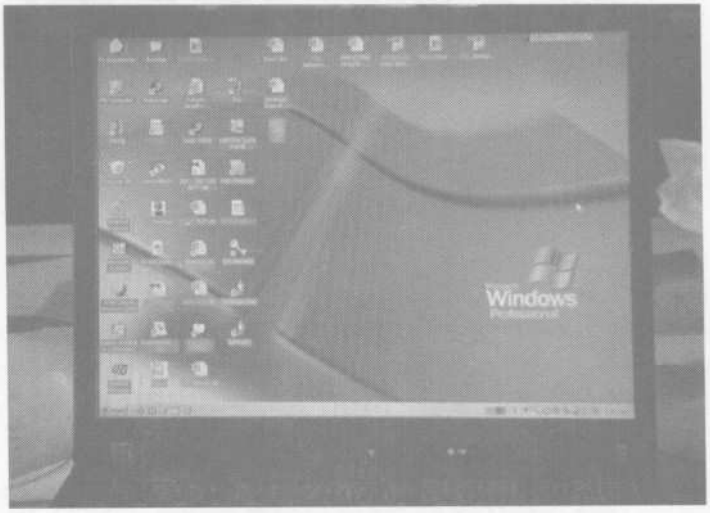
很抱歉直接引用了《指环王》（Lord of Rings）里的对白，不过甘道夫（Gandalf）说的没错，保护私人物品不让别人享用。不要在公共场所处理私人事务，并且注意不要让自己成为目标。注意正在处理的文件，如果必要，把它隐藏起来。如果必须在公共场所工作，那么考虑使用笔记本计算机防偷窥滤光镜（laptop privacy filter）。当然，一个有经验的偷窥者看到滤光镜后马上就意识到你正在处理敏感信息。正因滤镜才使你及计算机成为了目标。不要在公共场所处理私人事务，这才是最佳选择。

电子推理

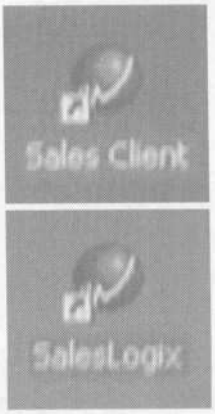
信息显然比硬件珍贵，专业的盗窃者是很清楚的。尽管业余的盗窃者可能从计算机的使用时间以及硬件标识来判断计算机的相对价值；而专业的盗窃者通常会观察机器使用者的情况，再使用非技术手段来检测存储在机器中数据的价值。我们已经知道了一些有趣的外部线索，但观察用户的最好方法是看显示屏。

StankDawg（http://www.stankdawg.com）发表了一篇题为《电子推理艺术》（*The Art of Electronic Deduction*, http://www.docdroppers.org/wiki/index.php?title=

The_Art_of_Electronic_Deduction）的论文，文中探究了攻击者从感兴趣的电子设备上搜集信息时使用的方法。先读他的文章，认真查看下面的照片，我在咖啡店里拍到的一台无人看管的笔记本计算机，屏幕上的信息一览无余。

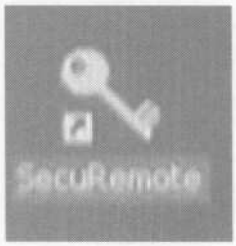


为了保护机主公司的信息，我已经处理过图片了。但是，利用屏幕中的信息，一个经验丰富的非技术黑客能够收集到相当多有用的信息，而新手可能只会注意到桌面背景，知道机器上运行的是 Windows XP 专业版。对技术黑客来说，操作系统是必要的信息，他们可以借此决定使用哪种攻击方式。一般说来，攻击者需要分析一系列的网络数据包才能确定操作系统的种类，但这种情况下就不必了——因为机主不太可能使用其他操作系统的桌面背景。再关注桌面上的图标，一个图标就把用户工作的公司的相关信息清晰地暴露了。我们能从下面的图标中得到更多的信息。



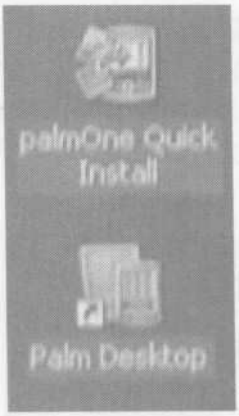
单词“销售”（sales）表明了这是某种销售管理软件，用 Google 搜索可以发现，SalesLogix 是用户关系管理（customer relationship management, CRM）的主流软件。搜索结果还告诉我们 SalesLogix 是“网络上最强大的销售工具”。我们可以很肯定，机主在销售部门工作。下面的图标涉及 SAP，这是一个普通的商业软件方案提供商。

SAP 客户端图标暗示了登录验证信息可能也安装在计算机上。假如黑客准备对机器下手，利用存储在计算机中的信息就能够进入公司的 SAP 系统。下面的图标为 SecuRemote。



用 Google 搜索后知道，SecuRemote 是种虚拟专用网络（virtual private network, VPN）客户端。加上 SAP 注册软件，VPN 验证信息可能全部或部分存储在计算机里，黑客可以很轻易地进入公司网络。至少，仅仅是某种特定 VPN 的存在，就已经为黑客提供了宝贵的信息。

下面的图标则表明机器安装了个人数字助理（personal digital assistang, PDA）软件。机主可能拥有一部 Palm 设备，而设备中的内容很可能在计算机中有备份或与计算机中的内容同步。

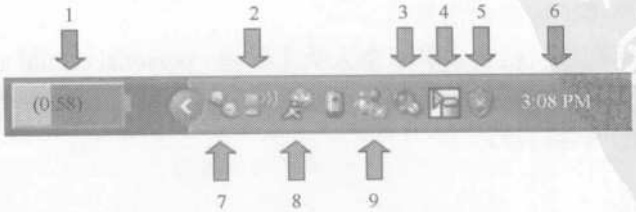


下面的图标表明计算机安装了 AT&T 全球网络客户端（Global Network Client）。

网络客户端可能缓存了一些验证信息，这可能会使入侵者以机主身份登录。如下图，这个图标的命名不太合适。

我只希望文件没有包含任何类型的实际登录密码。如果那样，入侵者也太走运了。

桌面图标提供了很多信息，但一个聪明的攻击者看屏幕上的一些细节便能得到很多信息。例如，通过观察下图中的任务栏图标能得到什么信息呢？



任务栏本身告诉我们很多信息，布局显示了此 Windows 版本很可能是 Windows XP。但每个图标含义不同。你认识多少？下面是各个图标的含义：

1）电量指示器，表明设备是笔记本计算机，还剩余 58min 的电量。还可以知道，设备没有接电源，因为没有看到充电图标。

2）机器正在连接无线网络。

3）此图标表明机器处于静音状态。

4）IBM 硬盘驱动器活动保护程序图标。表明机器是 IBM 的。

5）微软安全中心当前没有运行，意味着安全级别不高，很容易遭受攻击。它也是机器运行 XP 系统的又一证据。

6）显示系统时间 3:08 PM。与当地时间联系起来，判断机主所在时区。若未设置，表明其产地。

7）Trillian 即时信息程序。Trillian 网站（www.ceruleanstudios.com）描述这个程序是“功能全面、特点鲜明、皮肤可更换的聊天客户端，支持 AIM, ICQ, MSN, Yahoo Messenger 及 IRC”，是一个即时信息客户端的替代产品。图标风格显示 Trillian 已连接登录。

8）AIM（AOL Instant Messaging）图标，已经建立连接，用户已经登录。

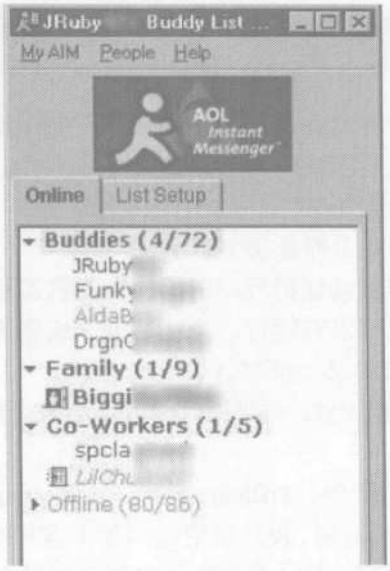
9）MSN 程序正在运行，但用户没有登录。

10）看似奇怪，他同时运行 Trillian，AIM，MSN，有 Trillian 存在，AIM 和 MSN 就多余了，很可能是出于使用偏好或某些其他原因。确切的事实是，这些客户端在线提供了观察员调查研究的平台，因为 MSN 和 AIM 都要求用户注册之后才能使用，并建立个人形象，其中可能包含个人真实信息。在绑定软件和创建在线形象方面，雅虎即时通是目前使用最多的。所以，雅虎的用户要格外小心，不要将太多个人信息暴露在网上。

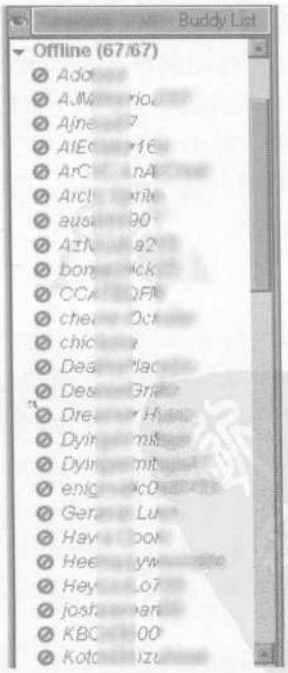
即时通信工具里的陷阱

关于在使用即时通信软件时如何保护隐私，我们可以专门写一本书。当注册获得账号后，新用户创建了许多数据，这些是黑客日后能找到的线索。由于页面上的空间有限，我们不再深入讲解所有的陷阱，只要读者明白一点，如果关心自己的隐私，注意即时通信客户端上填写的信息。

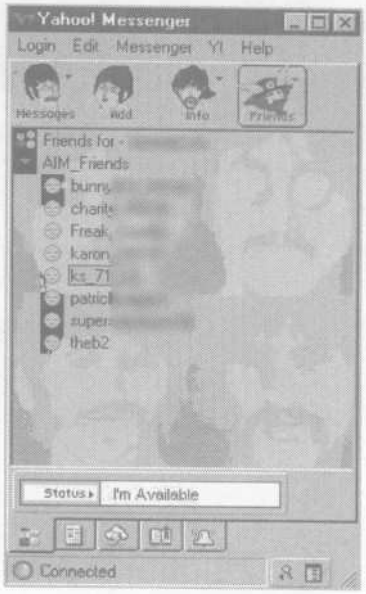
一个关于即时通信软件用户的在线调查显示，每个用户必须有一个用户名。如果一个聊天窗口如下图所示登录，用户名就会显示在窗口顶部。



有了登录用户名，黑客可以在网上搜集机主的信息及好友信息。有一串好友名单，如下图所示（StankDawg 提供），黑客可以深入挖掘从私人注册信息开始的所有个人信息。



有时候，好友名单不如好友列表本身重要。如下图所示（StankDawg 提供）。



很显然，该用户是个披头士迷。一个社会工程师能利用这个信息开始交流。正如 StankDawg 所言，黑客能发现大量信息，有些内容看似无用，但当这些星星点点的信息通过各种各样的资源（屏幕摄像、肢体语言、穿着打扮、行为举止等）汇聚到一起的时候，偷窥者能建立起让人惊讶同时又很精确的目标形象。

但任何通过这种方式构建的形象都可能有瑕疵，这点非技术黑客很清楚，他们不会指望这些信息发挥什么巨大作用。考虑扩展工具栏里的东西，如下图，即时通扩展版的图标，我们在上文中讨论过。

还有很多有趣的图标没有显示出来，但箭头指示的那个很明显。洋葱头代表 Vidalia，一个合并了 Tor（The Onion Router）和 Privoxy 的工具包，这两个工具可以使用户在上网过程中保持匿名身份。用户在使用 Privoxy Tor 工具浏览网页的时候，可以保持完全匿名状态。远程网页服务器无法确定用户来源，嗅探本地网络流量工具也同样不能确认用户来源。这个小图标不超过 40 像素，却告诉机主的很多信息。这是个不知道 AIM 和 MSN 区别的用户，实在有些愚蠢，尽管他（她）采取了一些保护措施，但还是面临威胁。这种推测可能是错误的，但最出色的非技术黑客可以从这些细节中精确地提炼出真相，然后根据真相做决定——这个过程只需很短的时间。

注释

最好的防御就是在旅行时保持警惕，不要在容易被偷窥的环境里使用计算机。使用计算机的时候背靠墙，随身携带计算机。不要穿带公司 Logo 的衣服。去掉额外的标记和信息，特别是当公司名字比较明显的时候。公司的技术人员能提供避免发生这种情况的技术手段，应该听听他们的建议。

电子推理绝对是门艺术。关于这个题目有很多内容可以讲，但想想我们此刻收获了什么——事实上，计算机屏幕上的每个位置都有非技术黑客感兴趣的东西。如果计算机上有吸引小偷或非技术黑客的东西，不要暴露在公开场合。不要让自己成为目标。

偷窥实战

军事机密

只有非技术黑客把想法付诸实施，才知道他们有什么想法。这一部分，我们看一些现实世界里背后偷窥的场景，第一个例子就是下图中的小伙子。

很明显，他在军队服役。他的制服上的徽章已经透露了很多信息，尤其是有点军事常识的人。某些人可能因为他是军人才对他有兴趣，但任何非技术黑客都

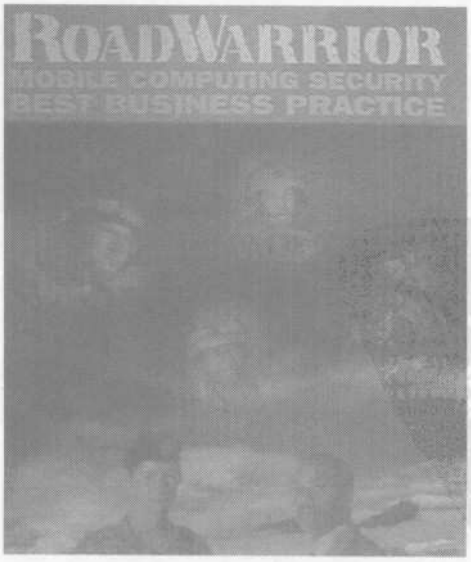
会从他身边的设备得到很多信息。

即便是新手也能看出他是苹果公司的用户。他用的是苹果的 PowerBook，白色的耳机上有 iPod 标志。屏幕下方苹果爱好者杂志揭示了他是一个苹果爱好者。再进一步分析，他还是个游戏玩家。

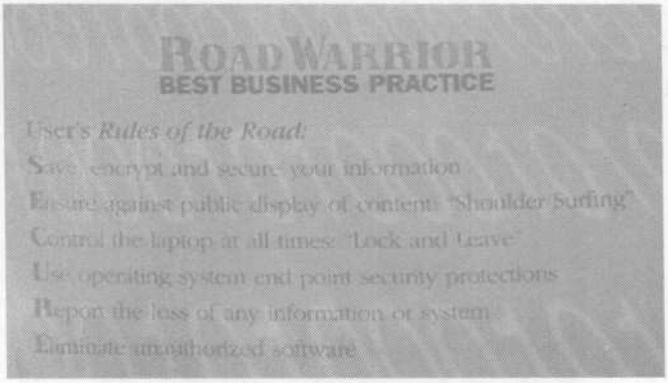
任务栏里的小图标表明他安装了魔兽世界和 Ventrillo 语音通信软件。

社会工程师可以利用这些信息，如邀请他一起玩魔兽世界或进行语音聊天。但大多数非技术黑客会避免使用社会工程技术，除非万不得以。我们只需再走近一些就能知道更多。

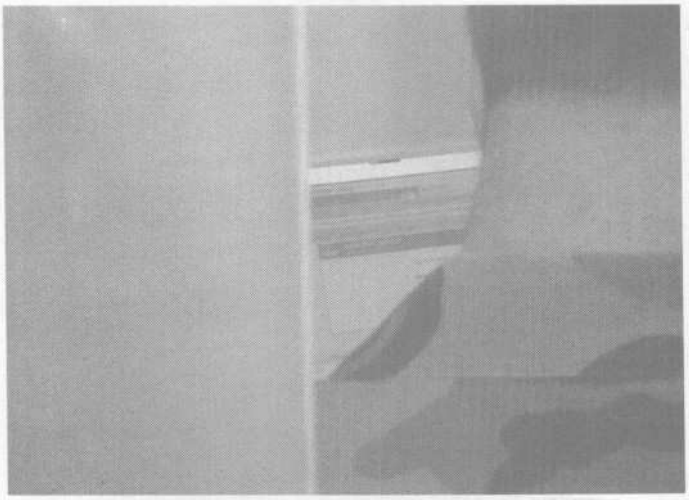
我不得不承认，很惊讶能发现这样的目标，把后背暴露给大家，而且带着耳机，不禁想到了最近发现的“马路勇士”（RoadWarrior）。



在“马路勇士”的卡片上有一些提醒，包括“不要在公共场所显露，防备背后偷窥者”、“做一个谨慎、机警的旅行者”等。



然而，如下图中看到的，靠近这个小伙子很简单，因为他戴着耳机，还坐在对着墙角的位置。



结果发现，他不是在浏览网页——他正在登录 BEA WebLogic 服务器的管理员控制台。WebLogic 是一个很有分量的企业级软件，他在紧张地工作，可能与美国政府有关。在他录入口令等信息的时候，我又拿出了另一个相机。闪光灯一闪，他马上转过身来，这才发现了我。我低头看着相机，揉了揉眼睛，假装被闪了眼睛。他耸了一下肩膀又继续工作。他竟然相信了我，我觉得他认为我是一个新手，还不太会使用数码相机。他当然没注意到我在拍他。当然，这样做会给他带来很多麻烦。如此看来，他和许多笔记本计算机用户一样，会把问题往最好的方面考虑。这就使非技术黑客的工作变得更容易了。

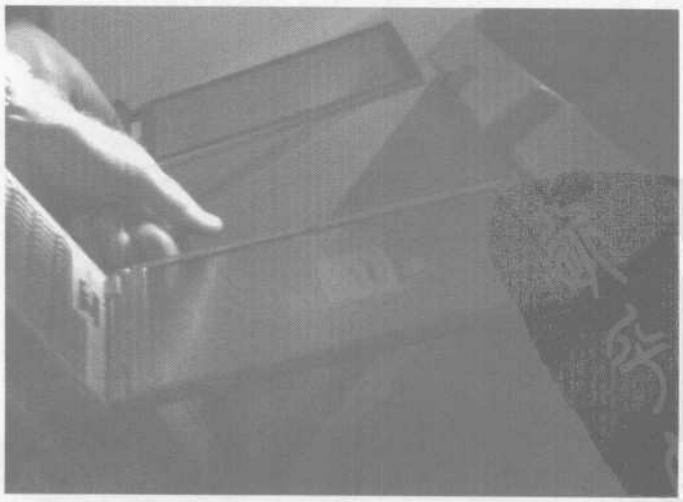
扔掉！

我不建议和可能在偷窥的人进行肉搏，但我觉得应该在感觉到自己被偷窥的时候关掉机器，装作对别的什么事情感兴趣，如喝咖啡。这时，多数非技术黑客会明白他们被发现了，会马上走开。如果他们还是和以前一样，就要留意一下了，当他们走开的时候仔细观察他们的车或其他特点。当他们彻底消失的时候，看看刚才所做的工作，并且假设所有的东西都暴露了，想好应对之策。如果那个人还在跟着你，那就死死盯住他。如果很可疑，马上采取一些措施，如通知大厅经理、保安或门卫，总之做点什么。如果涉及暴力事件，不要告诉法官是我的主意。

航班间谍

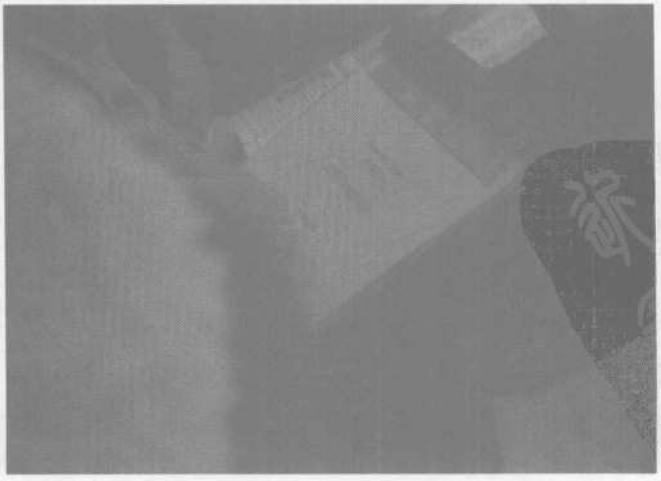
下面的例子发生在30 000英尺高空中的一架客机上。客机上进行背后偷窥很难，因为偷窥者通常受到座椅的限制，不方便看身边及过道边的乘客。

我在旅行的途中从来不睡觉，要知道没人能在睡觉的时候进行非技术入侵。深夜，我醒着的时候看到了发生在另一排的一幕，那是一个远程会议。起初，我并没有太在意，因为坐在靠窗的位置，身边的乘客一直醒着，在喝浓咖啡。我一直准备着，当身边的人起身去厕所的时候，马上按下了快门，拍下了下面的照片。



这个照片拍摄的角度太差了，但打量机主之后，我意识到他的举止动作很像在政府部门工作的人。他的文件夹肯定是政府部门的。我偷偷瞥了一眼他的计算机包，上面有政府部门的某种标识。我又装作不在乎地观察了一会儿，直到他回来。他回来坐好后，拿起一本杂志开始看。我关了相机，试着找别的什么东西。尽管刚才做得非常好，但偷窥毕竟也是一项很累的工作。如命中注定，这次行动并没结束，而是刚刚开始。他打开笔记本，开始处理一些文件。从旁边拍摄文件有点困难，但我用夹克形成一个临时的幕布，挡住相机，然后调整焦距，抓拍。没人注意到我的行动。

他在处理很多文件，这让我很兴奋。尽管我不是政府人员，但知道他的工作应该很重要，而且他好像并不在乎有人在看他。我很乐意接受这种邀请，最后瞥了一眼文件头，那里有很多信息。我忍不住又把相机拿出来拍了一张。



页面上用大号标题写着“政府系统 EW/SIGINT 2006 战略计划”。任何业余的 Google 使用者都能告诉你“EW/SIGINT”是军方对电子战信号机密（Electronic Warfare Signals Intelligence）的称呼。我感到心跳加速，我意识到自己在 30 000 英尺的高空正在偷窥什么。我马上停止拍照，动作没有太反常，因为现在知道如何使他们的电子系统瘫痪，就使用这样一台廉价的相机和一盘磁带，尽管有时我老婆还抱怨机器噪音大。

抢银行

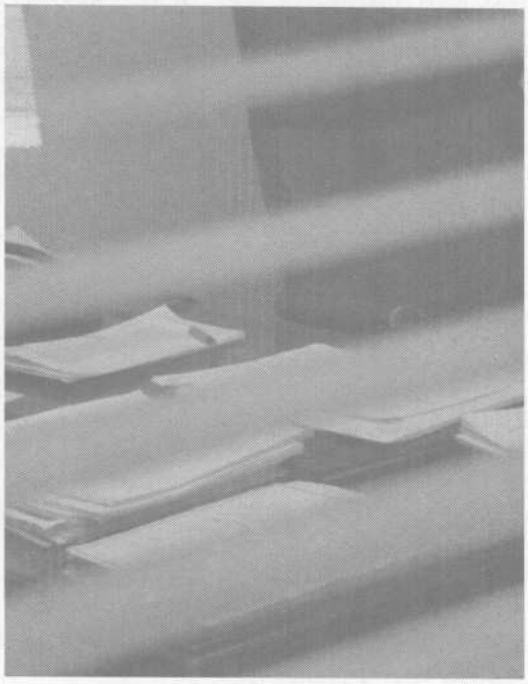
银行有电子和物理安全系统，安全系统等级高达 5 级。但我在银行里学到的是：即使最好的安全系统也有共同的一个缺陷——懒惰的人。拍下这个照片时，我确实没有抢银行的打算。

当我走过前门时，瞥了一眼坐在拐角处办公室里的银行经理，他正在使用计算机工作。我停下脚步，转身透过窗户看着他。虽然他就在我的正前方视线里，却没看到我。我拿出相机，退一步，拍了下面的照片。

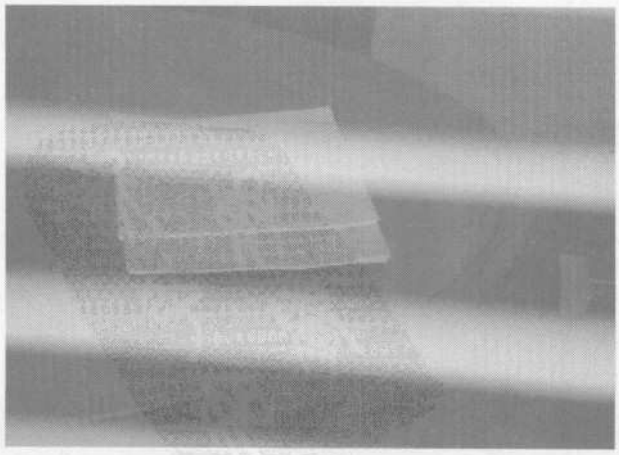
很明显，由于我的出现，他向周围看了看，又继续处理文件。我仍站在原地，拉近镜头，对着他的屏幕拍了一张。看了照片，发现照片中屏幕上的字看不清楚。经理仍在工作，所以我就调整了焦距（花了点时间，因为我很少这样做），接着拍了几张。最后拍的照片可以很清楚地看到屏幕上的字（照片已经过后期的模糊处理）。

我站在那里，在相机的液晶屏上看银行经理的屏幕的时候，感觉偷银行的钱很容易。银行拥有的信息比实际流动资产有价值的多。专业的罪犯和小偷之类的人可以很轻松地弄到银行的数据库，从而得到实实在在的钞票，比洗劫大厅或劫

持人质的风险小多了。我想知道一屏有多少客户的个人信息。当我想到如果我是一个坏人该有多富有时，那个经理起身离开了办公桌，此时办公室没人，我调整焦距又抓拍了几张他桌上的东西。最后焦距很合适，我拍到了一张清晰的文件照片。



我从来没想过对于一个非技术黑客来说盗窃银行的信息会这么简单。我又拍了房间里其他地方的几张照片，如下图所示。



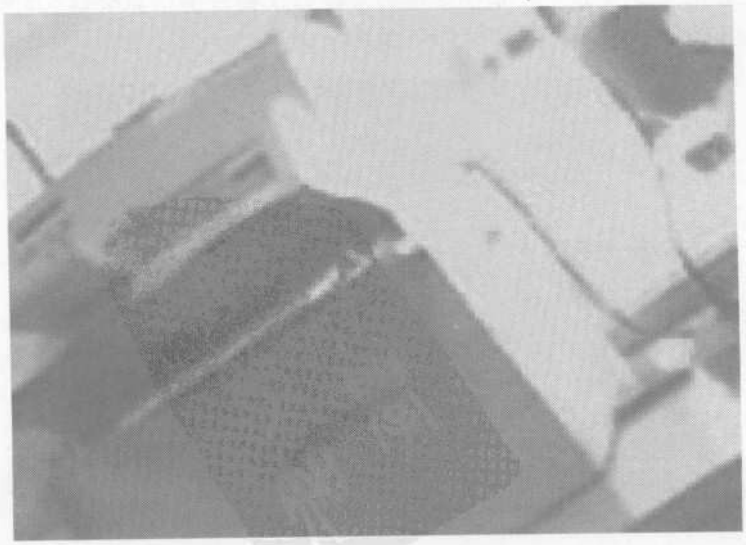
看了看照片，我发现它们都很清晰。一会儿，经理回来了。我站在那里手里拿着相机，对准了他的办公桌，我在想如果把手头的信息拿去卖，估计还可以支付我的保释金。他还是没注意到我，慢慢走到桌边，调整了腰带和裤子，一屁股坐在椅子上，都没瞟我一眼。

我有点紧张，害怕被银行的警卫注意到，但什么也没发生。我转身继续走过办公室，差点撞到一个在抽烟区吸烟的银行职员。他没看我一眼，忙着打手机，而且就在经理办公室外面。我突然意识到，原来经理对窗户外的人来回走动已经习惯了（包括拿着相机的我），他都没觉得有什么威胁。警卫通常盯着监视器好几个小时也没什么异常。他们已经习惯了什么都没发生，因此当一些事情发生的时候，他们往往注意不到。

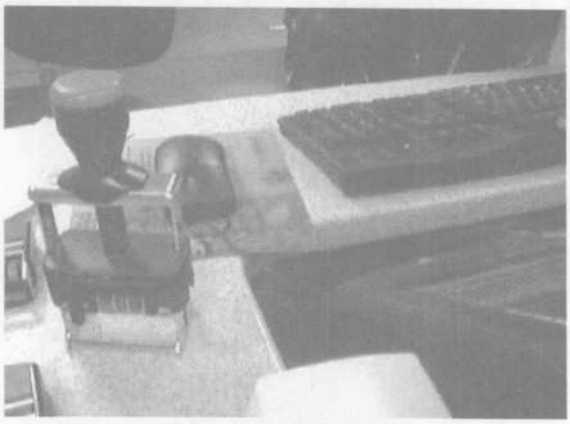
我能复制这些照片吗？

不行。我再重复一遍，我不是坏人。如果我是，那么肯定会很富有，住在 Cell Block 13 区（富豪居住的地方）娶芭芭拉为妻。但我不是，我是一个高尚的人，只是要提醒这些部门提高安全意识，尤其是非技术手段的威胁。

后来有一次我去银行办事（合法的），在站在出纳员桌边的时候，偷偷地看柜台后的设备，用手机拍下了下面的图片。



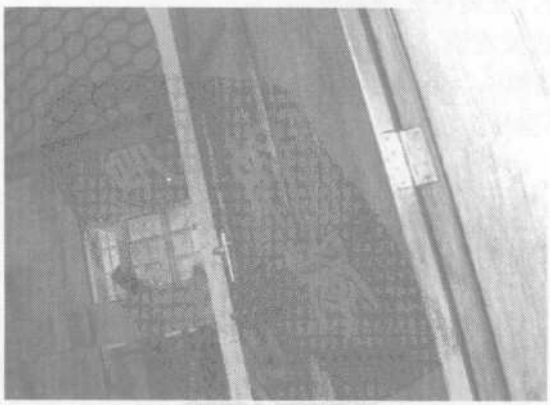
这张小小的、模糊的、大幅修改过的打印机照片没什么可看的。实在是不好意思，我用它出于两个原因。第一，现在在任何地方都有可能拍照片——包括在机场候机厅，虽然那里有武装警卫到处巡逻，还写着“禁止拍照”警示牌。



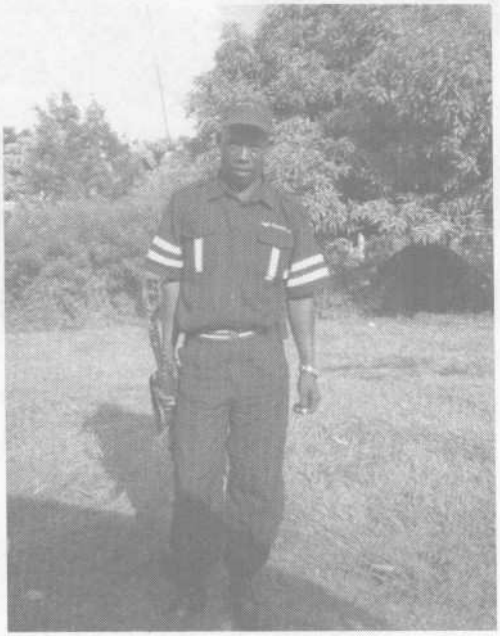
第二个原因并非打印机本身，而是机身上方贴的标签，上面清清楚楚的写了这家公司的名称、电话。银行使用该公司的产品。如果觉得打扮成计算机修理工只是电影里的情节，再想想现实中有没有可能。我已经成功地做过很多次。我做过之后甚至根本不了解谁是真正的 IT 售后公司。

在乌干达抢劫银行

最近有去乌干达的任务（参考 http://johnny.ihackstuff.com/uganda），当时我都没有非技术攻击的想法。和在美国的家乡相比，那里完完全全是另一个世界。但当我站在 Jinja 最大银行的自动取款机前的时候，惊讶地发现银行使用一种特殊的铁具锁门，它像篱笆一样固定在门上。我觉得很有趣，就拍了下来。



当我从相机里看拍的照片的时候，脑子里尽是这种装置潜在的安全威胁。碰到这种装置，我的顾问 Vince 可能已经有很多方案来攻克它。通过使用衣架的小伎俩就可以打开门，遮挡安全摄像头监视，或者……这时有人推了我一下，把刚才的想法打断了。一个满脸怒容的男人，手里握着一把看着挺吓人的来福枪，站在我身后。“禁止拍照，把相机收起来”，他嚷着。

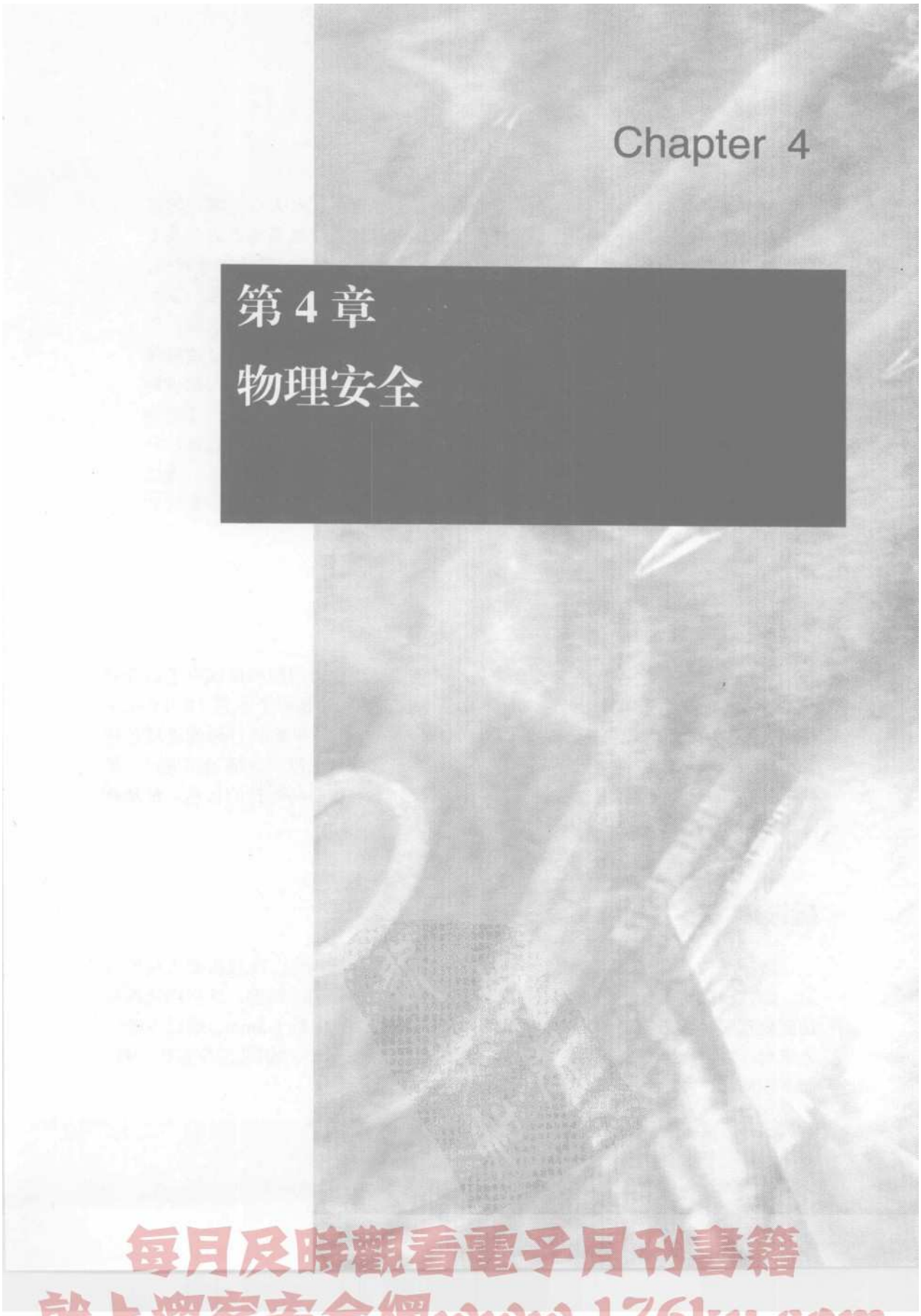


来福枪让我很震撼，他身上的制服更让我难忘：帽子和领子上有公司的标志“Tight Security”。很有讽刺意味的是，我在一个许多人认为是第三世界的国家里，却碰到了可能是所见过最好的安全防护。我扫视四周，马上发现还有 3 个守卫，相似的武器和衣着，在银行外围巡逻。

“你好啊”，我笑着说。

那守卫的表情严肃，没有笑容，说到：“把相机收起来。”

我低头发现手里还握着相机，于是清清喉咙，把相机放了起来。



Chapter 4

第4章 物理安全

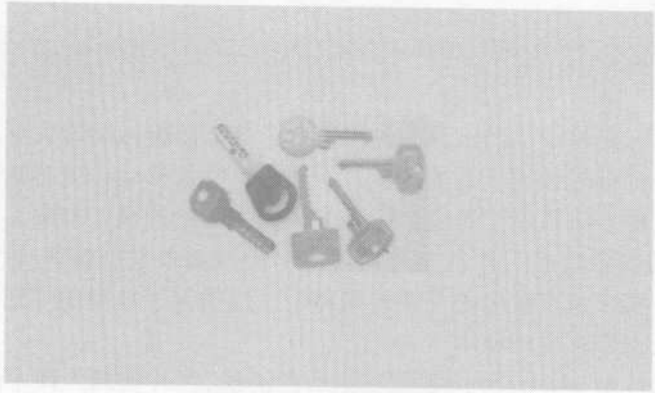
锁在实际生活中扮演着重要的角色，这方面的技术人员是真正的工程师，他们大多数功底深厚，有多年的实践经验。当德高望重的锁具专家遇到天才黑客，猜会发生什么？神奇的事情就会发生。曾经信赖的锁，已经沦为非技术工具的受害者，而这些工具仅仅是钢笔、金属丝、卫生纸卷之类的东西；号码锁可以保护财产，锁上的密码有数万种组合，但有人不借用任何工具不到 3min 就能打开；行李箱上的锁是经过政府相关部门检测的，却败给了用苏打水罐做的铝片和塑料条；最让人惊讶的是枪上用来防止误伤的保险栓竟可以用吸管灵巧地挑开。锁一旦遭到这样的攻击，我们还指望摄像头、动作传感器、警报系统做些什么呢？只能眼睁睁看着他们得逞。有点夸张了？事情就是这样。我相信，看过本书中内容最长也是讲解最深入的章节后，你会对安全领域的现状有点担忧。

引言

我还记得第一次进行系统安全评估时的情景。我挑选门锁和调试电子监视系统，想象自己是电影《异形》（Aliens）中的哈德森，也就是那个水兵（Bill Paxton 扮演），尽力维护电子仪器正常工作以保证船员的安全。虽然我曾经闯进过各种各样令人惊叹的地方并绕过了一些电子监视系统，却从来没有靠撬锁实现过。最简单的技术从来不会过时，在这一节中，我将分享一些非高科技的技术，都是新老黑客常用的手段。

撬锁

撬锁是门技术活。不仅要知道锁的机械原理和内部构造，而且需要大量的练习。撬锁已成为非技术黑客的必修课。需要学会使用专门的钥匙，这些钥匙都被切割处理过，留下很深的痕迹，顶部和侧面用锉去除了大约 0.5mm。通过专业眼光来看，专业人员撬锁用的钥匙和一般的钥匙明显不同，这些钥匙刻痕都很一致，如下图所示。



使用这种钥匙开锁的过程是这样的：先将钥匙插入锁内，然后一边将钥匙往外拉一边慢慢地转动钥匙。锁芯转动，慢慢将带动弹子。当上面的弹子向上移动，下面的弹子仍在下面。当内外弹子分离时，圆柱体的锁芯就可以转动，如果动作准确，锁就打开了。用这种钥匙开锁比以前的撬锁工具简单，甚至比电子开锁仪也简单，不需要多少技巧。这就意味着任何人只要拥有一把这种钥匙，就有可能打开锁。如何做好防护，以及什么样的锁易受攻击呢？想要知道更多信息可以查看相关参考资料，或者与专业的锁匠和安全服务提供商联系。

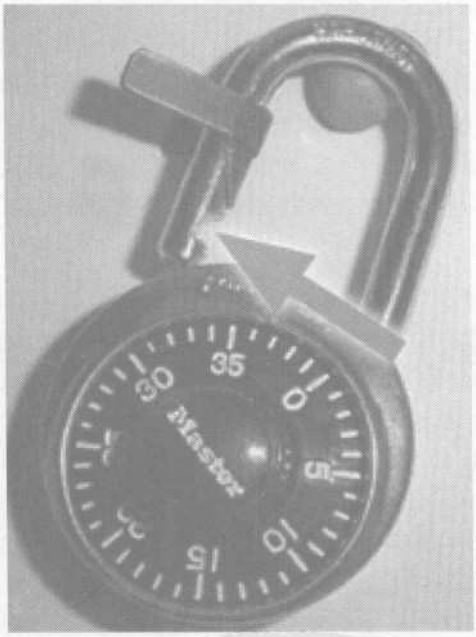
撬锁的奇妙之处

撬锁这种方法其实很早就有了。而最近的一些作品使得它更为人们所熟知。Marc Tobias 的《锁、保险柜与安全》（M.W. Tobias. Locks, Safes and Security: An International Police Reference Two Volumes, Charles C Thomas Pub Ltd, 2000.）是很好的专业参考书，书中介绍了许多关于如何撬锁的知识。他的网站（http://security.org）以及警示网页（http://security.org/dial-90/alerts.htm）上也有很丰富的资源。如果正在寻找这方面的资料，建议看 *Bumping Locks*（http://www.toool.nl/bumping.pdf），作者是 Barry Wels 和 Rop Gonggrijp，他们都是开锁者开放组织（The Open Organization of Lockpickers, Toool）的成员，他们以"What the Bump"为主题的视频研讨会在网页（http://connectmedia.waag.org/toool/whatthebump.wmv）中展示。Toool 的网站（www.toool.nl）上有许多资源和视频资料，强烈推荐下载观看。

填塞挂锁

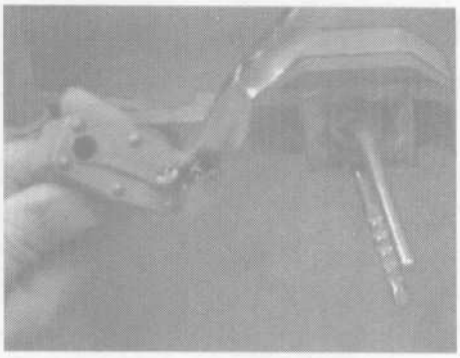
填塞的含义是将细小的工具塞进锁芯内，使锁的机械装置失灵。一个铁制或铝制薄片如果能插进锁内合适的区域，弹子就可能被移动，锁芯就可以转动，从而打开锁。这种方法只能打开完全依靠弹簧压力工作的锁。本质上说，填塞好像使得保持锁的安全性的工作落在使用者的身上。如果使挂锁关闭需要让锁栓入位，那么填塞挂锁重点要做的是让锁栓移位。这类似于典型的“信用卡”攻击：在上锁的门闩上来回滑动信用卡。

下面的照片是 Master 号码锁被填塞后的情景。薄片被插入锁中的滑动锁芯与固定部分之间，这种情况下通常能把锁打开。



确定一把锁能否被填塞处理的方法有很多。最简单的方法是在锁打开的时候，用一些如凿子之类的小工具刺进锁洞内。如果锁芯可以被轻易地转动，那么它内部是使用弹簧的，容易被填塞。如果觉得这样很难理解，我更简明地描述一次，这没有什么难以理解的。

有的锁在两侧都有锁孔，如下图所示。这样的锁可以很容易被探测和填塞，即使有两个锁孔，但它只有一个普通的锁栓来调节锁身，因此不管锁的哪面朝前，安全性是一样的。

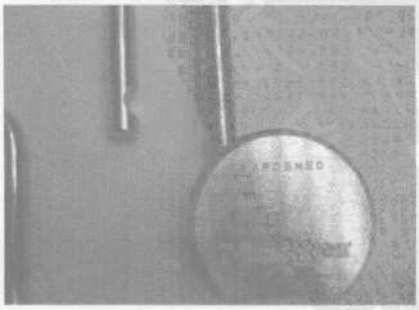


如果一个锁有两个不同的锁芯，加塞就困难多了。由于挂锁自身的构造特点，直接对这两个锁芯进行“戳测试”不太可行。但测一个锁芯就足够了；如果锁一边是用弹簧制动的，那么另一边很可能是一样的。对这种锁进行加塞处理的关键是必须用两个夹片，一个凹槽一个。这样做可能遇到问题，从商店买回的弹簧铁太厚，也就是说攻击者必须用一些较细的工具，如铝条（可以用可乐罐或啤酒罐制成）。

我能给你提供什么呢?

黑客和啤酒罐有什么关系？当然，他们用铝制的啤酒易拉罐制作出很好用的铝条。制作简单，但用起来很棒，为避免此书成为犯罪分子的技术指南，下面这个链接介绍一些独特的方法：www.i-hacked.com/index.php?option=content&id=189。

确保对锁进行这种攻击测试。业余人士很难确定一把锁是否可以被加塞处理。下图中的 Master 锁很常见，在大多数的商店都可以买到。有句话说的好，一分价钱一分货，这种锁用的是双球机械装置，它是不能被加塞的。



下面是打开防填塞型锁的一些技巧：

1）一把锁可以锁上，但不需要钥匙或号码组合，那么内部通常是装有弹簧的，容易被填塞。

2）如果锁的钥匙在使用锁的过程中始终固定，那么这种锁一般不易被填塞。

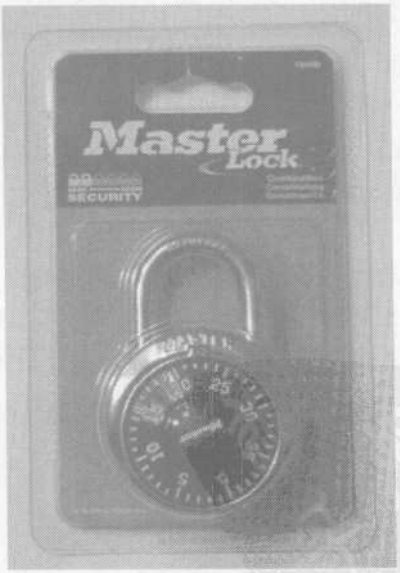
3）锁的外包装上有“双保险”型装置的广告，大都不能被填塞。

4）挂锁的设计主要是防止断线钳的破坏，一般很难被填塞。不仅难于填塞，它的典型特点是质量好，机械设计出色，能提供较高的安全性。

5）相信锁匠推荐的某几个牌子的挂锁。如来自 Sargent & Greenleaf 的 8088 和 8077 系列的锁，这些类型的锁是用在国防部的文件柜上的，经过双重认证。

Master 号码锁

我还记得小时候看到很酷的 Master 牌锁时的情景，哪怕用工具把它穿透也无法打开。对我来说，Master 牌子的锁已经是安全的代名词。直到今天，许多买 Master 锁的人都是冲着牌子去的。然而，不要仅靠牌子买锁，因为各种牌子的锁设计的安全级别是不同的。一定要仔细调查这些产品以选择适合自己使用的锁，如 Master 1500D 型的号码锁很畅销。



该公司却没有将它作为高安全性锁，而是在多数基本的安全应用中推荐使用这种锁。我基本能天天看到这种锁，尽管它时时面临蛮力攻击的危险。

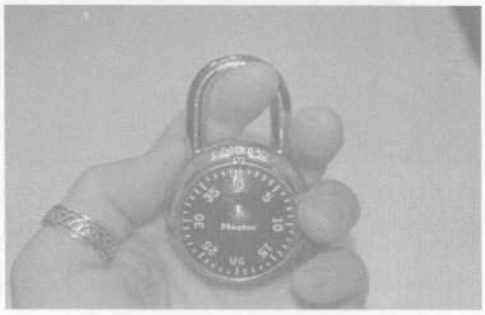
蛮力攻击描述这样一种技术，就是为了找到解决办法去尝试每种方法。例如，

对于一个由3位密码组成的号码锁，所有可能的组合是从000～999，如果一个人从001，002，003开始尝试，并将每种组合试一遍，蛮力攻击保证可以在1000次以内打开这把锁。大部分的号码锁都可以通过蛮力攻击的手段打开，但需要攻击者有足够的耐心，这也就是该锁所能提供的安全级别。

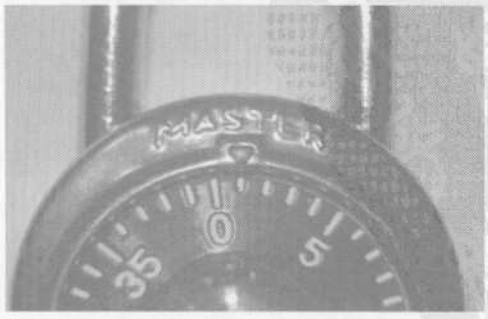
事实上很多人没有足够的耐心通过蛮力攻击的方式打开号码锁。假如现在有把Master牌的号码锁，而假设转盘上的号码是可以动的，留给我们的是40^3（即64 000）种组合。如果一个攻击者每5s尝试一种可能（考虑到合理的速度，以及清除和旋转的动作耗时的因素），他可能需要长达88h的时间，也也就是接近4天的时间才能全部尝试完。在这种情况下，被累垮将会是攻击者，而不是锁。

我会告诉你一个技巧，可以将所有可能的组合降到100以内。每种尝试用时5s，只需8min就可以试完100种组合。鉴于本书是介绍如何保护财产的，我不会深入讲解这种方法的细节，但我会告诉如何确定数字组合的最后一个数字。如果发现组合数的第三个数字，那么换个更高安全性的锁吧，或者最好找个专业的锁匠来评估锁的状况。

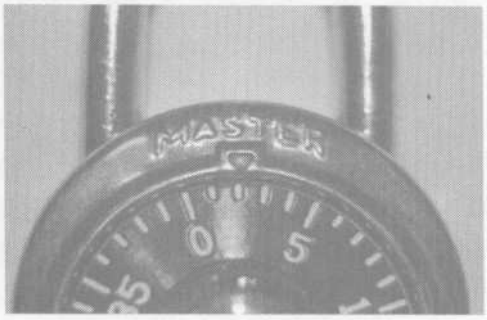
首先，用力压锁的顶部。一种简单的做法是用一只手握住锁身，同时用一根手指用力从下往上顶锁的上部，如下图所示。当然图中时髦的戒指不是测试必须的。



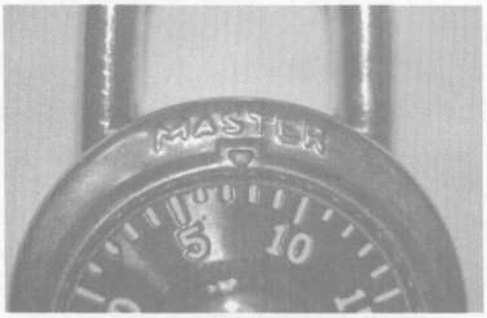
接下来，开始旋转锁盘。如果力量足够大，锁盘将在两个数字间停留。我称作“粘滞点”。每个受到影响的锁上存在12个粘滞点。第一步是找到并记录每个粘滞点的位置。例如，这把锁的第一个粘滞点最低位置如下图。



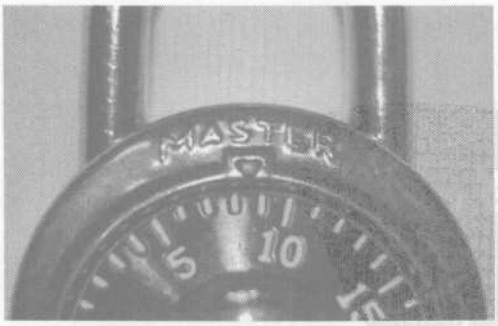
该点的最高边界在 2 处，如下图所示。



二者之间是 1.5，不是一个整数。再找下一个粘滞点，放松，转动锁盘，经过当前粘滞点的最高边界后再加压，锁盘会停滞，显示出第二个粘滞点。有时粘滞点可能不是整数，下图中显示了一个粘滞点的最低边界位于 7.5。



我意识到你们（善良的读者们）明白我所讲的内容里没有这些图片，但是让我们再看看这张，已经包括了奇数、偶数、高位和低位粘滞点。高位边界在 8.5，如下图所示。



这就是说，粘滞点在这个位置。通过记录每个粘滞点，将得到和下表类似的东西。

表　锁的粘滞点

低位边界	高位边界	粘滞点
1	2	1.5
4	5	4.5
7.5	8.5	`8
11	12	11.5
14.5	15.5	15
17.5	18.5	18
21	22	21.5
24	25	24.5
27.5	28.5	28
31	32	31.5
34	35	34.5
37.5	38.5	38

注意有超过一半的粘滞点并不是整数。这些是圈套，应该从所有可能的数字组合中除去。在这个例子中，剩下了五个数字：8，15，18，28 和 38。注意到这些数字大都在同一个数字处结束——数字 8。这些匹配数字也应该从列表中删除，只留下一个数字（15），就是我的号码锁的最后一位数字。

如果这种方法也适用于你的号码锁，那就意味着你的锁也可能会遭受蛮力攻击的袭击。如果没有效果，可以换个新点的 1500D。据检测序列号以 800 开头的 Master 锁不易遭受这种攻击（见网页 www.wikihow.com/Crack-a-Master-Combination-Lock），尽管没有证实这些新锁是否会遭受攻击。无论如何，先不要急着唾弃 Master 锁。做研究，不要在高安全性的任务中使用低安全等级的产品。要记得购买高安全级别的 Master 牌锁，或从专业的锁匠或安全部门得到一些建议。

获取真实信息

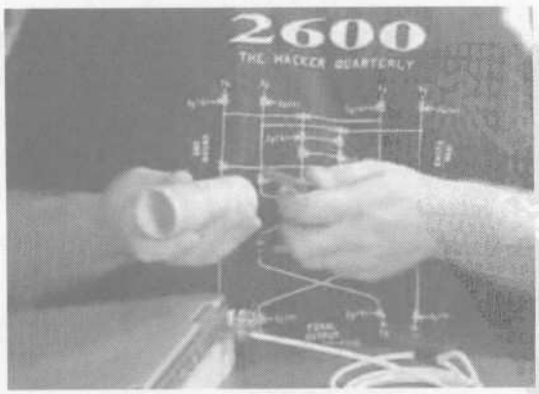
有一些网站详细地讨论过这个弱点。然而，确定组合数的前两个数字牵涉相当数量的数学问题和记忆问题。Tim Mullen 给出了一个捷径，在《网络盗窃》（*Stealing the Network: How to Own a Shadow*，由 Tim, Ryan Russell 和我合著）一书中讲述了一个故事，内容是黑客在实际生活中擅长干什么。当然，故事是虚构的，但其中的技术手段，如对 Master 牌锁的蛮力攻击手法却是真的。细细阅读书中的内容，了解黑客“金盆洗手”后会做哪些事情，有哪些是在现实生活中容易遇到的。

厕纸与管状锁

管状锁的应用范围很广，最常见的是笔记本计算机锁，如下图所示。

1992 年，英国广播公司（BBC）报道，一些管状锁容易被小偷避开，而失去作用，并且他们不需要多少技术就能做到。12 年后，2004 年 8 月，Marc Tobias 发现 Kensington & Targus 公司生产的笔记本计算机锁中使用了类似的圆柱轴设计。他在报告中指出，这种设计可以用一支钢笔甚至厕纸卷轻松地打开。2004 年 9 月，Chris Brennan 在他的论坛里（www.bikeforums.net）描述了如何用一支钢笔打开昂贵的 Kryptonite 自行车锁（这种锁使用的也是圆柱体轴设计）。Chris 把视频传到 www.bikeforums.net/video，接着媒体的报道接踵而至。

当 Barry 出席一个黑客会议时，他制作了一个展示如何运用搭桥技术破解特定的 Kensington 笔记本计算机锁的影片（http://www.toool.nl/kensington623.wmv），并在会议上进行了播放。黑客社区发现这个视频很有趣，但一般市民不敢相信这是事实，他只用厕纸卷里的纸板就可以在很短的时间里成功做到。



虽然总是有猜测谁先想到什么，已经有 100 万人从 Barry 的网站上下载了这段视频，还有其他无数人从 YouTube.com 网站上观看。我爱 Barry 的视频，因为它清楚地说明了我在本书中所强调的，即使是最复杂的安全系统也有可能受到简单攻击的威胁。如果你的笔记本计算机里有敏感数据，并且只靠一个锁定装置保护这些数据，那就要注意了。只依赖单层的安全保护，迟早会受到攻击。使用笔记本计算机锁不是一个糟糕的主意，但如果担心计算机上的敏感数据丢失，就应该考虑一些加密解决方案。总之，应该从黑客的角度思考问题。以这种方式考虑，一根细长的电缆线是最好的解决办法吗？

电动开锁器：低科技含量的杰作

撬锁确实需要技巧。要正确的操作，不仅需要知道锁内部的机械原理，还需要大量的练习。随着新工具（如撬锁枪之类的电子设备）的出现，开锁变得比以前容易了。然而，这些工具操作不简单。要正确的操作需要一定的技巧。另外，它们价格昂贵。相信大多数的业余人士不愿花钱购买一个不太容易操作的专业设备。

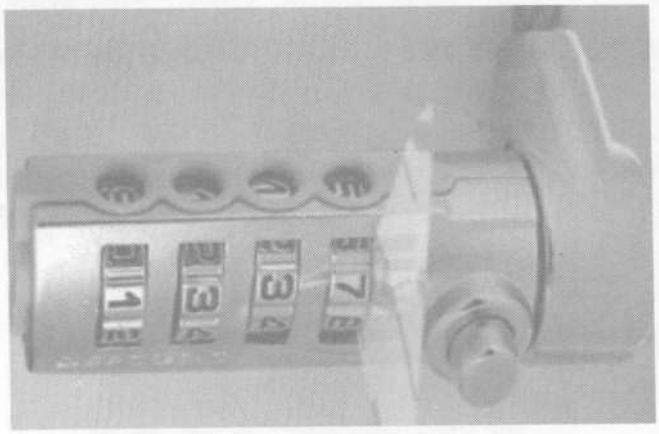
但是一些小的黑客工具却比较有吸引力，撬锁社区里有很多新鲜的电子小玩意，如下图所示。

我不清楚是谁想出了这个主意，用这样一个东西作为黑客工具，但还是有人做了。做出的结果就是这样一个微小的、廉价的电动开锁枪。根据 Jared Bouck 在 inventgeek.com 网站上所介绍的，这个小东西，若再配合一把钳子，能在短短的几秒钟内将锁打开。

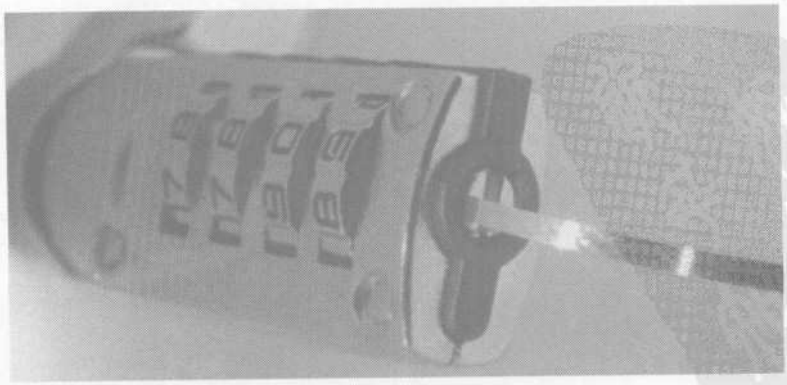
通过改造可以让装置获得更强的动力，将它插入锁内时，可以有足够的旋转力撬动锁。务必访问 www.inventgeek.com 得到更多的信息，以及务必抓住任何偷偷使用这个工具的人。他们绝对在做什么见不得人的事情。

啤酒打败笔记本计算机锁

许多号码锁容易受到攻击，常称为“探测门”攻击。这种技术需要使用一个小塞片，它用来探查号码锁的锁轮位置（如下面的照片所示），以找到“闸门”或开口，这将揭示组合的内容并最终打开锁。2004 年 8 月，Security.org 报道说 Targus Defcon CL 的“计算机电缆锁”（PA410U 型）容易受到这种方法的攻击。

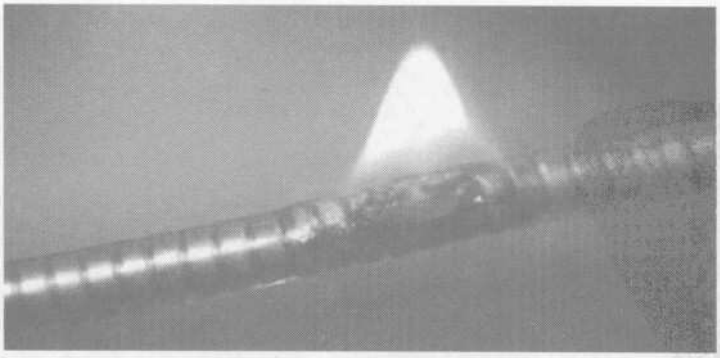


因此，Targus 对锁进行了重新设计来规避这种风险。新锁（ASP10US 型）使用了新的装甲电缆。经分析验证，Targus 已经纠正了最初的问题，将阀门移动到内部。然而，人们发现一种新方法使锁更易受到探测，只需探测锁身末端的组合螺杆的变化。这项技术将允许攻击者探测阀门（一次一个圆柱），但为了成功实现这一攻击，需要去掉塑料外壳或用一个非常薄的垫片滑过外壳。



下面该啤酒罐登场了。这种攻击需要一个厚0.015英寸（约0.38mm）或更薄的长条。物理安全专家Matt Fiddler和Marc Weber Tobias发现从啤酒罐上切割下来的铝片厚度仅为0.005英寸，非常合适。

但对这种锁的研究还在继续。Mike和Marc发现电缆本身可能受到攻击。为达目的，要先将电缆外层包裹的塑料去掉。如下图所示，打火机可以快速地除去聚氯乙烯薄膜。

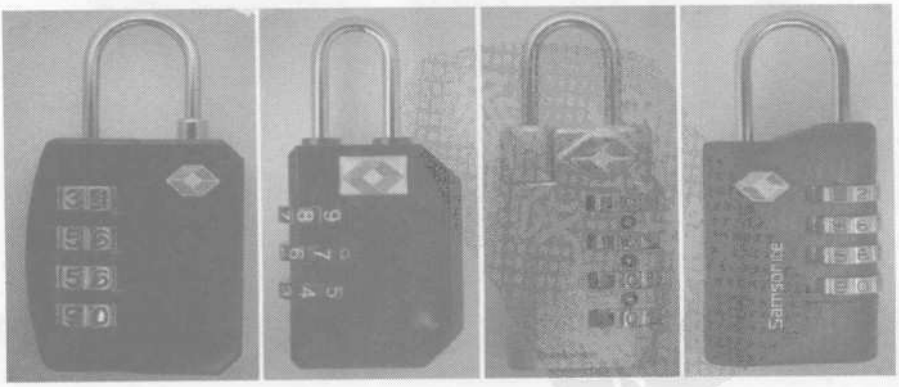


除去外面包裹的聚氯乙烯薄膜，只需用普通的钳子就可以把锁切开，如下图所示。

这些测试告诉我们，在挑选任何安全设备的时候要提高警惕，尤其注意笔记本计算机锁。计算机里的信息往往比计算机本身有价值。投资要明智，测试要准确。使用任何安全设备之前一定要测试。

TSA 锁

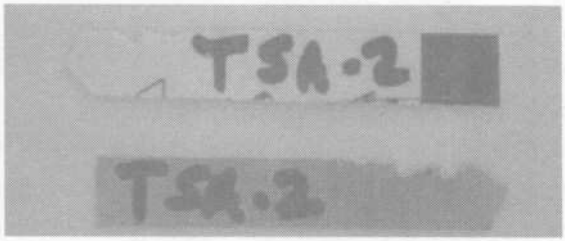
9.11 事件后，机场加强了安全检测，交通安全管理局（Transportation and Safety Administration, TSA）禁止在旅行箱上使用普通锁，但允许使用“TSA 锁”。这种锁旅客可以锁上，TSA 工作人员可以打开并重新锁上，而不必麻烦旅客告知解锁号码。如下图所示，这种锁在全球的机场行李站已经很常见。



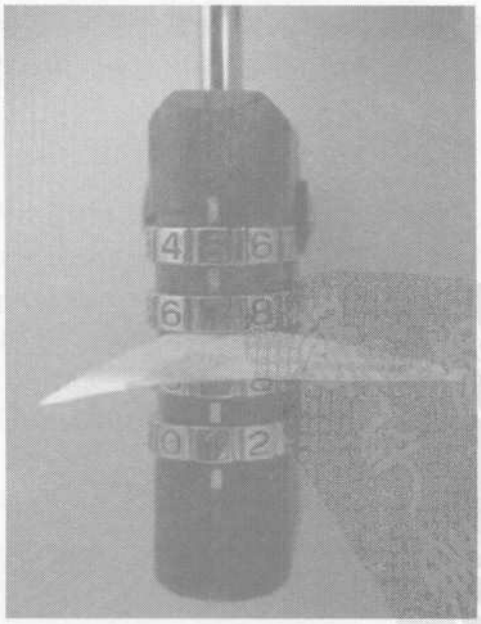
Marc Weber Tobias 对这种锁进行了审查，并把结果公布在一份题为“交通安全管理局核准的行李锁”（http://download.security.org/tsa_luggage locks_ report.pdf）的文章上。他的结论是非技术黑客可以梦想成真了。他概述了锁本身的弱点，并且指出，大多数行李箱上的锁很容易被打开，所以不必使用这种锁：

> 测试的每种机制都不需要使用任何特殊的工具或专门技术，而且仅需很短的几秒钟就可以把行李箱打开。旅客们不能指望使用这种锁保护自己的行李。虽然行李问题专家指出，通过切割外层物质，绕过拉链，行李箱可以很容易地打开，但真正的问题是由走私或过晚的察觉造成的。本报告审查了每种类型的锁，以及在非法入侵时的脆弱性。

Marc 发现，许多锁可以使用简单的金属或塑料片打开，如下图所示。



他的论文还描述了如何在 TSA 锁上使用门探测技术（如用于打开 DEFCON CL 系列锁）。通过一些塑料片，就可以一次确定一个轮子的数字，从而打开密码锁。



在某些情况下，对手可能需要进行一些简单的加减法，以确定锁的真正密码，但我们谈论是二年级的算术，而不是代数。

SploitCast 的合伙人 Ross Kinard 很不喜欢 TSA 锁：

> 由于 TSA 锁大多都是需要口令的“芝麻开门”型的锁，也继承了其他同类锁的问题。其他类型的锁可以被拆开，以研究主键的键值深度是多少。根据我的经验，当键值调整到一定幅度时，用任何一块金属都可以开启 002 位置，可以把它固定在键槽中，再进行微调。在 004 只需要一个坚硬的小金属片转动（内凸轮），随 007 产生的号码对所有其他 007 的也有作用。

Marc 的最终判断是确凿无疑的：

> 很显然，交通安全管理局批准的锁提供不了所需要的安全。用户必须面对的问题是“行李需要什么样的安全保护？”答案显然不仅仅是锁的问题，也许行李的安全永远不能真正得到保证。
>
> 这项报告的结论很简单：不要依靠这些锁提供任何级别的安全保护。它们仅仅是一种形式昂贵并可以重置的装置。有些相关知识的人可以通过解码打开这些锁，并不需要什么训练和专业知识，而且人们可以在任何地方买到这些锁，所以盗窃之前训练不是问题。当然，锁使安全保护工作变得相当简单，但允许任何能接触行李的人来打开它。

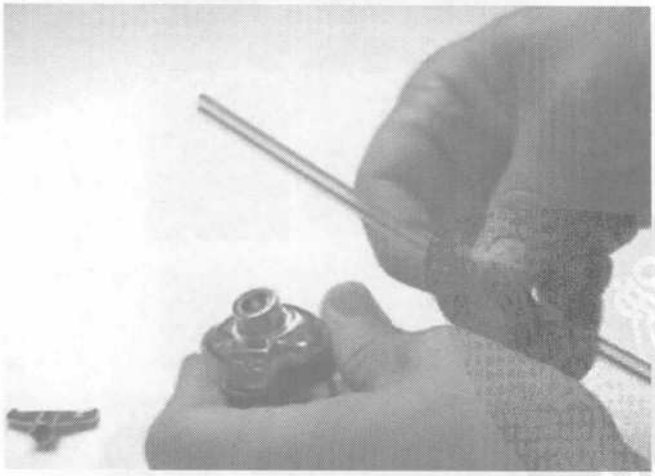
我们赞同专家所建议的：想想行李箱里装的东西，是否会引起任何有企图的人的注意。随身携带不可以丢失的东西，并且记得时刻保持警惕。

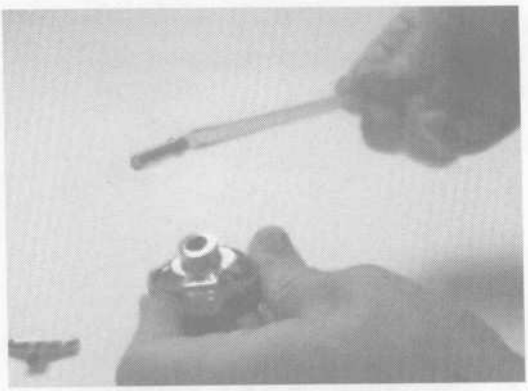
枪锁与吸管

当我坐下来考虑书中提到的物理攻击中的非技术黑客手段，从来没有考虑涉及枪锁。因为工作中很少碰到枪。但是，由于 Marc Tobias 和 Matt Fiddler 的良好声誉，我采用了他们的《枪锁报告》（http://download.security.org/ gunlock_2007.pdf）。令我感到惊讶是，它绝对是一个非技术的黑客手段，在这里我大致列一些出来。虽然我认为不必完整在这里描述它，但觉得有必要帮助他们将报告中说明的枪锁系统的内部隐患告诉大家。如果有任何在本章节中描述的枪锁，立即用更安全的产品替换它们。

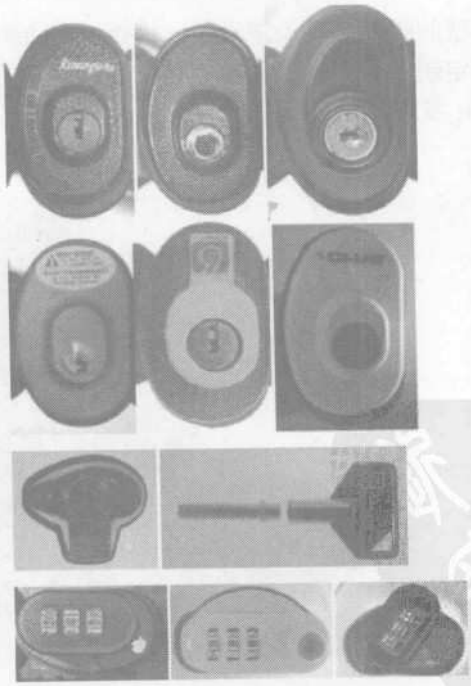
最可笑的攻击集中于 DAC 扳机锁。如下图所示，它可以在许多零售店买到，包括沃尔玛（Wal-Mart）、凯马特（K-Mart）等。

这种锁有一个典型的折叠式整流罩设计，将扳机和防护装置包裹起来。锁的安全性一半是由与特定钥匙匹配的螺纹栓提供的。在锁定的位置，栓的顶部凹入锁身内。Marc 和 Matt 发现，用麦当劳的吸管可以比较容易地打开这种锁，如下面两张照片所示。



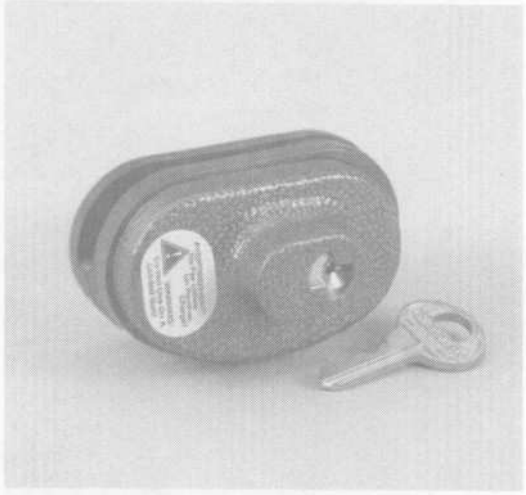


Ross Kinard 补充说，与锁配套的钥匙用锉打磨一下就可能打开其他 DAC 枪锁。报告接着说，许多其他品牌的枪锁也很容易受到威胁，包括某些 Master 锁、Remington 和 Winner International 锁，其中一些小孩子用冰凿或螺丝刀就可以打开。事实上，每个扳机锁（如下图所示）都有严重漏洞，如美国司法部的“儿童安全项目”钢缆枪锁；Master 的 90、94 和 106 型扳机锁触发模锁；DAC MTL 的 100 型扳机锁；Franzen 号码锁；GSM 的枪扳机锁和温彻斯特（Winchester）枪击案等。



美国消费者产品安全委员会在其网站上（http://www.spsc.gov）列出一份召回

明细单。许多责任厂商（如 Master）都召回他们的产品，例如，某些 90 版本的锁具（如下图所示）。可以访问 cpsc.gov 的网站查看被召回的型号，确保你的锁没有问题。在此，我不做任何评论，这是一个非常严肃的话题。



枪支安全

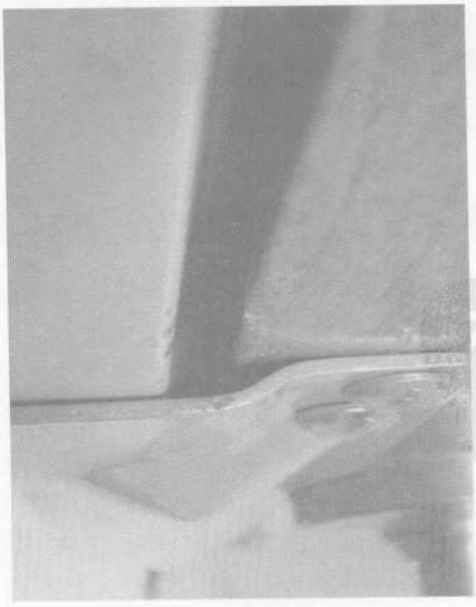
如果你有枪，应该为它们安装质量过硬的扳机锁，并锁在柜子里。保管好钥匙并保持警惕，确保武器的安全。最重要的是，请专业锁匠对安全措施进行评估。

进入技术：万能锁卡

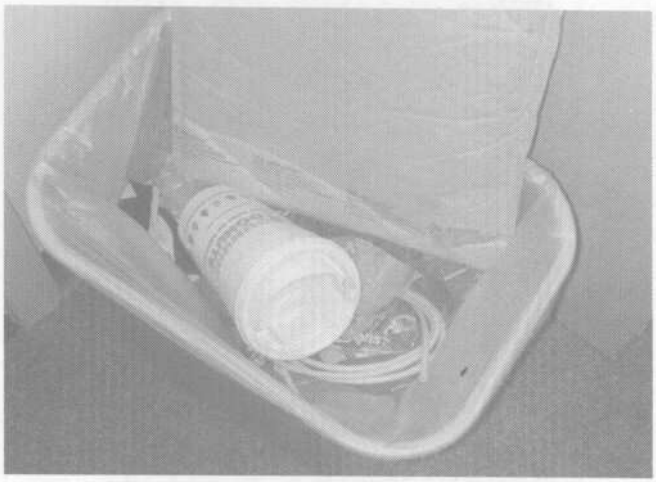
好像每个人都知道信用卡的秘密。事实上，只要条件合适，这种开锁手法一般人不需要培训就能够做到。不过，似乎每次我都很走运，因为总是能成功。这个方法又叫作使用万能锁卡，运作方式很简单。要穿过一扇锁着的窗口，攻击者可能会尝试在窗口处滑信用卡（或结实的细线），将插销打开。要穿过一扇门，攻击者会用信用卡在门缝中来回滑动，试图将锁栓从锁槽里弄出来，把门打开（假设门上只有一个锁）。

门板与锁槽之间必须有空隙才能用这种方法。下图中空隙足够大了。

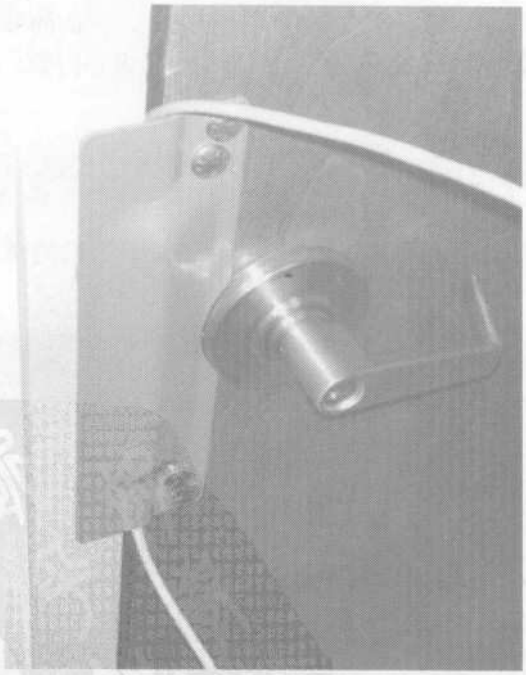
那不只是个门缝，甚至手指都可以轻松地伸进去，否则不会在上面加块铁板。但加个铁板并没有解决问题，从下面的图片中可以发现缝隙大到都可以用另一种工具来打开门了。



非技术黑客不会被这种安全措施吓倒。在环顾四周后，他会发现周围有个垃圾桶。



一个非技术黑客在确保垃圾桶里没有任何有用的文件之后，很可能拿起那小段网线。如下面照片所示，网线正好可以插入门缝。

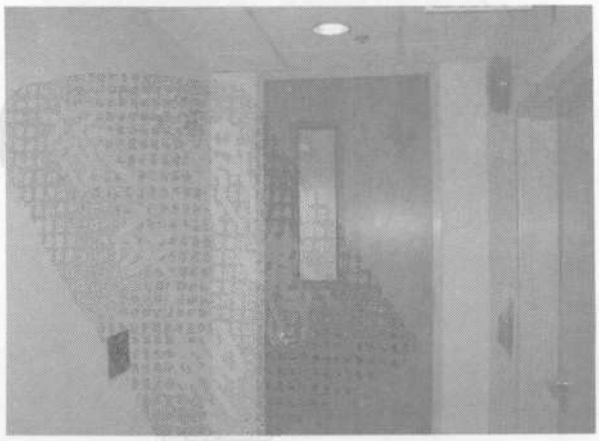


只需简单一拉，门就打开了。

我一直在想这种技术的使用频率到底有多高，因为记不清使用过多少次了，而且客户不愿意听到用这种小玩意测试他们的安全系统。留意关心的安全系统是否存在这种漏洞。当然，物理安全并非只与锁有关。下面的部分，让我们了解常被非技术黑客攻击的其他安全设施。所以不要过分担心门锁，还有更多需要关注的东西。

入侵技术：激活动作传感器

尽量不要在意标题中的动作传感器。现在，选择合适的角度，仔细查看照片中被锁上的入口。一个非技术黑客会选择攻击哪部分呢？



首先，墙上装了个读卡机。技术型的黑客可能想到复制一张卡或准备工具把它拆掉。我会用钳子和螺丝刀这类小工具来搞定。不过，这不是我们最感兴趣的方式。

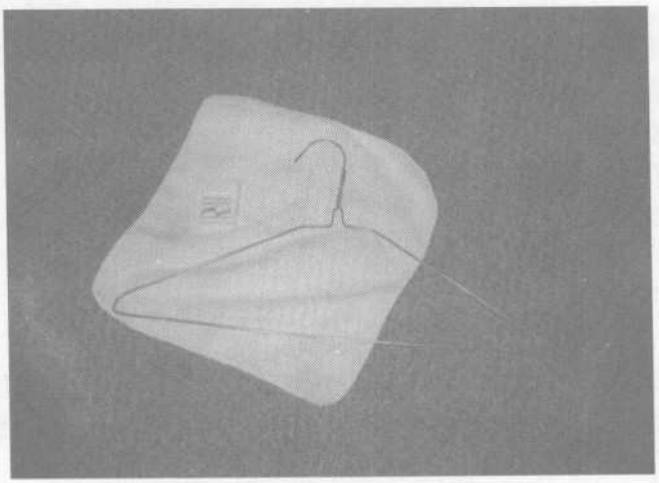
接着检查的是门框与门之间的距离。距离比较小，尽管门扳手可以清楚地看到，却不能用万能锁卡打开。比较温和的方式是利用社会工程方法从员工那里获取相关信息。我也想过尾随进入，但这些温和的方法可能会露出破绽，即便刚开始是成功的。最好的选择是等待和观望。员工肯定要从出口经过，这样非技术黑客可以观察到出门的过程。

如在前面提到的，Vince 告诉我，从楼里走出来通常比进去简单。每次我闯入有安全设施保卫的大楼，都会掂量这个建议。这次，那条建议在我等待了一段时间后应验了。一名员工从门里走出来，并伴随着刺耳的噼啪声。既然员工没有刷卡或拧门把手就能出来，问题来了：这是什么样的过程呢？从门上的窗里看，似乎能知道一点原因。没有看到推杆，也没有证据表明是门插销或按钮。门里的扶手几乎和外部的一样。问题的解答不在于看到的，而在于听到的，尤其听到的时间。

那种声音是磁性锁脱钩时发出的，很独特。有许多方法可以使磁性锁失效，但这并不是此次攻击的目标。目标是动作传感器，它控制磁性锁的开关。下图是从锁定区域的内部拍摄的，可以看到磁性锁和动作传感器。

一名非技术黑客是怎么知道有动作传感器的呢？两个原因：在员工走近门的时候它就开了，这可以从门中的窗口看到，员工没做任何动作，动作传感器做了这些工作。员工出门不需要任何特制的钥匙或进行什么操作。如果发生火灾，这种装置对于快速离开建筑非常有效。

一名技术熟练的非技术黑客可以轻松地破解这种系统，而且实现方法有很多种。为表达对 Vince 的敬意，我们使用下图所示的东西。



用些牙线将毛巾和衣架系在一起，然后做面旗，从门下面塞进去，来回摆动。最终引发动作传感器把门打开。测试出口程序的安全性。出口可能是敌人最好的入口。

用玩具打败动作传感器?

这当然是真的。一张白纸就够了，将它从门上划过或飘过传感器即可。如果做成纸飞机会更有趣。甚至用气球（长长的或者动物形状的）是很好的非技术工具。从门下塞进去，充气，来回摆动。不过，首先告诉人们在测试系统的安全性，不然他们开门撞到你的头就不太好了。

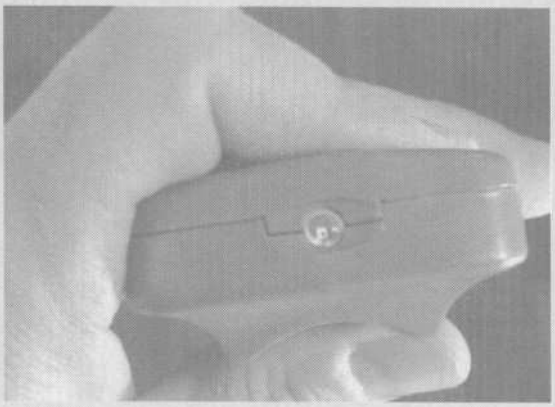
绕过主动式红外探测器

主动式红外探测器应用在许多复杂的报警系统中，但一些简单的系统中使用的探测器比较容易绕过。你看不到红外区域，因为它们不释放红外线。然而，它

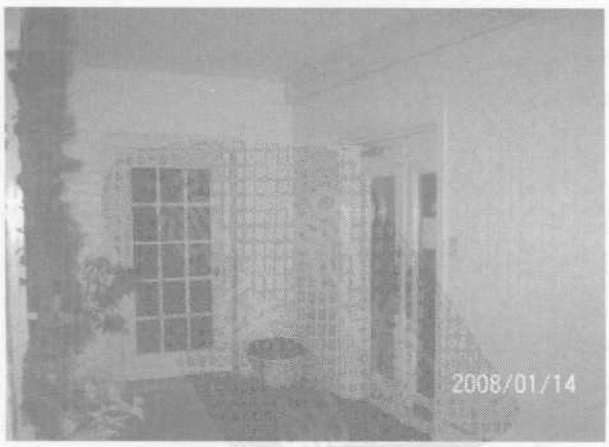
们能探测到红外能量，如人体发出的红外能量或者体温超过华氏 93°（约 33.9℃）的人。

观察红外线

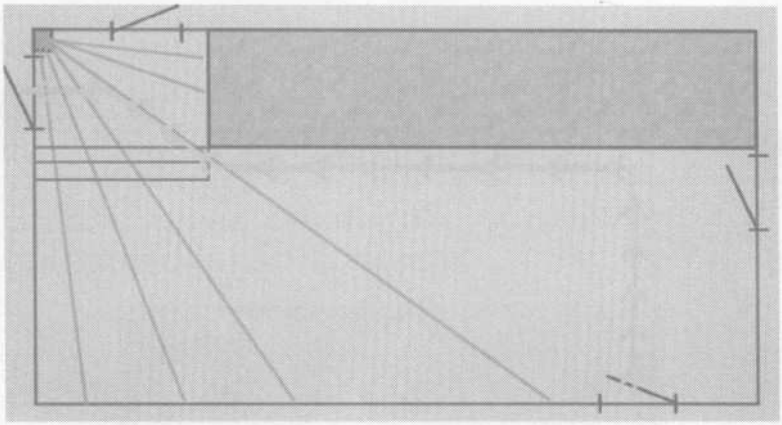
如果想研究红外线，可以用数码相机的取景器试试。电视遥控器发出的红外线平常是不可见的，这张照片是通过数码相机的取景器拍摄的。



这些类型的传感器在红外监视区域内不断变化，意味着它们可能被绕过，如小心翼翼地进入并通过监视区域。Ross Kinard 发给我一张照片，拍的是一个被主动式红外探测器监控的入口，监视装置安装在左边门口上。



罗斯在下图中画出了成功绕过探测器监视系统的过程。



既然传感器安装在了图左上角的位置，可以监视下面的两扇门，那么他从对角的门进去就不会被探测到。他走到对面墙边，沿墙根走，始终保持在监视区域之外。到达监视区域时，他很聪明地直接沿红外线束的方向走。这样，他就能保持轻快的步伐，每走一步花 4～12s 的时间。据 Ross 说，“那样做很容易。最难的是朝门口挪动的时候。那时我移动得相当慢，大约每次 2～4 英尺，每两步之间大约需要 6s，这个地方比较困难，因为不知道应该以什么样的速度通过，但最终我还是做到了。”

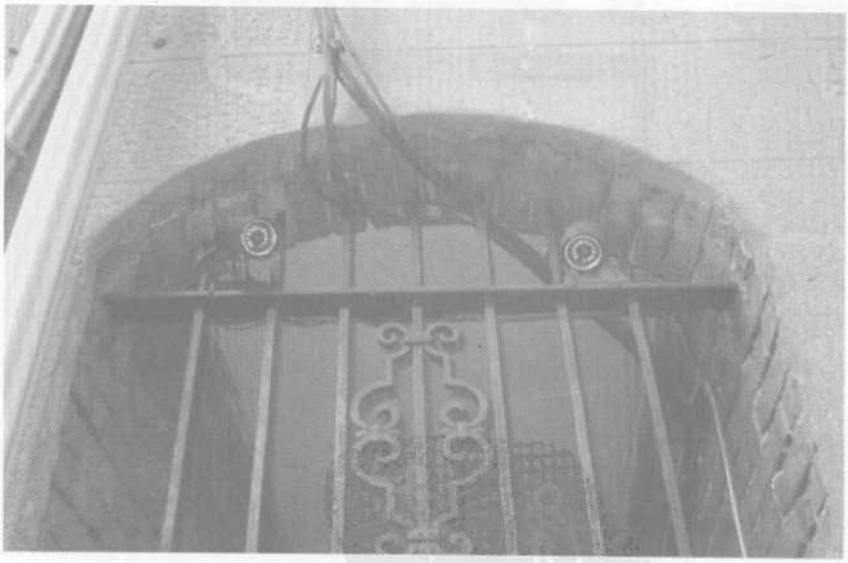
在我最喜欢的电影之一，《通天神偷》（Sneakers, 1992）中的 Martin Bishop（Robert Redford 扮演）为了对付一个动作传感器，穿了一身橡胶西装。他的同伙（River Phoenix）先将房间的温度升高到和 Martin 的体温差不多。然后 Martin 小心翼翼地靠近，最后成功避开传感器的监控。据探索频道著名的系列节目《流言终结者》（*MythBusters*）的工作人员介绍，片中的许多素材都是真实的。在 *Crimes and Myth-Demeanors* 第二部分（http://shopping.discovery.com/index.html）中，Kari、Grant 和 Tory 和一些安全设备较量，其中就包括红外和超声动作传感器。他们发现，“慢、低”技术对超声动作传感器也是行之有效的，这种传感器使用的是高频声波而不是红外线。他们还发现穿着橡胶服装可以在一段时间内使红外探测器探测不到攻击者。但最终由于衣服吸收了攻击者的体温，温度升高后就暴露了。他们尝试通过提高房间温度到华氏 98°（约 36.7℃）来迷惑红外探测器，但失败了，传感器马上就被触发了。他们曾用一块玻璃挡在传感器前面成功绕过监视，但前提是玻璃的温度和房间温度接近。最让人惊讶的测试是，Kari 用一个床单挡住自己，穿过超声波监视的区域而没有触发警报。

红外传感器被攻击的事件

在一个重大抢劫事件中（详情登录 www.crimelibrary.com/gangsters_outlaws/outlaws/major_heists/2.html），在营业时间内，一个聪明的小偷用有机硅喷雾器喷在红外传感器上，使传感器失明。有机硅涂层可以防止红外传感器检测热量的变化。

摄像机闪光

监视摄像机是最常见的一种物理安全设备。但是，许多监视设备设置得很不好，业余黑客都很容易躲过监视。闪光可以很容易地使摄像机失明或死机，使其不能记录任何有意义的东西。这些年，即使比较业余的窃贼也熟悉了这种技术，我却惊讶地发现它仍然在使用。Russell Handorf 是一名 CISSP（信息系统安全认证专家），向我提供了下面的照片，一个典型的摄像机安装图。



非技术黑客可能首先注意到，摄像机的数据存储部分和电源电缆暴露了出来，但电缆是用金属包裹的，很难切断。另外，相摄像机后的电缆集线盒是上锁的，不能移动。摄像机本身非常高端，是索尼的 Topica 型，TP-936WIR-30c 模块，配备 20 个 LED 红外夜视装备。

这个系统捕获的典型静态图像如图所示。

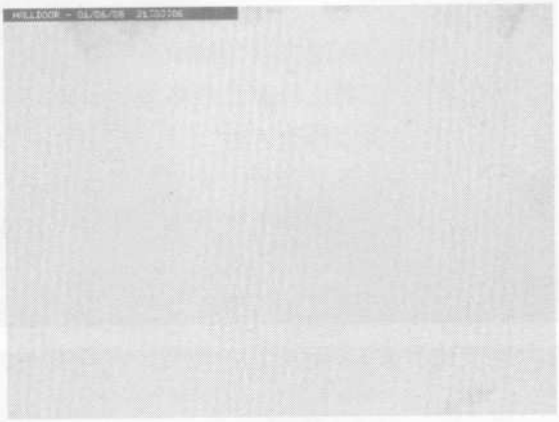
那么非技术黑客怎样攻击呢？我们称为摄像机闪光，就是使用异常强烈的光线让摄像机变成瞎子。下图中，Russ 用 SureFire x300 LED 灯发出强光。可以看到（或许看不到），用强光一照镜头里完全看不到任何东西。

这种技术允许攻击者出错。若没有用 SureFire 直接照射或直接照射的光线较弱，将产生一个类似的效果，如下图所示。

其他类型的光源也能这么做，甚至更远的位置也同样有效。看下面拍的图片。这个是我的脸。

使用激光发射器也会使它分不清我的面孔。如下图所示。

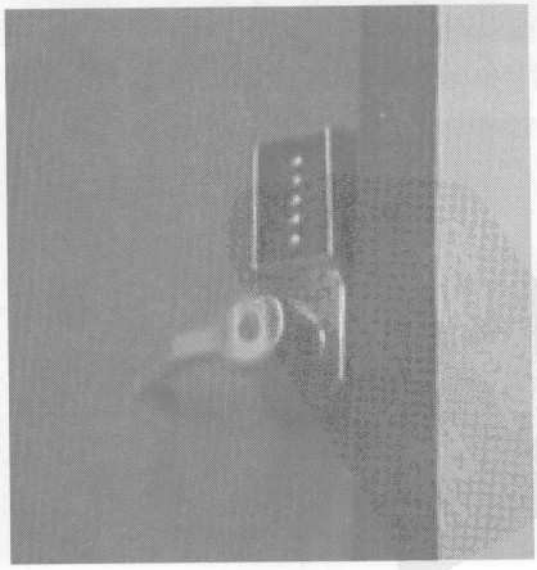
下图是直接击中镜头的效果。正如所看到的，照片中根本分不清是什么东西——摄像机完全瞎了。



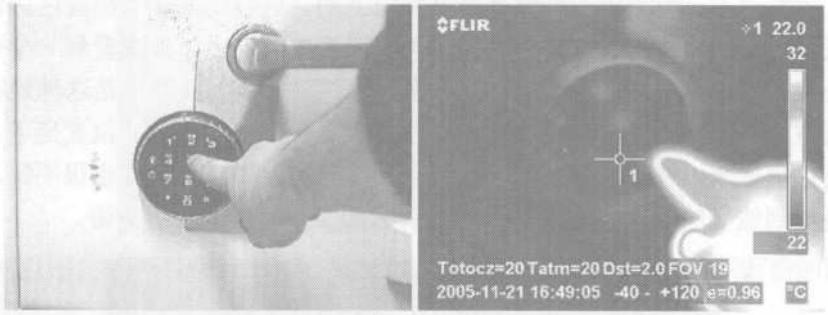
监视系统容易受到这样的攻击，可能考虑使用更好的设备，再安装一些摄像头覆盖更广的范围，或者考虑安装一台过滤器或反射装置来保护摄像头。记住一点，任何东西放在镜头前都会影响成像质量。在使用红外滤波器的时候要特别的小心。它们可能阻挡住夜间监视必要的光线，很大程度上影响摄像头的夜间监视能力。

现实世界：机场禁区单锁破解

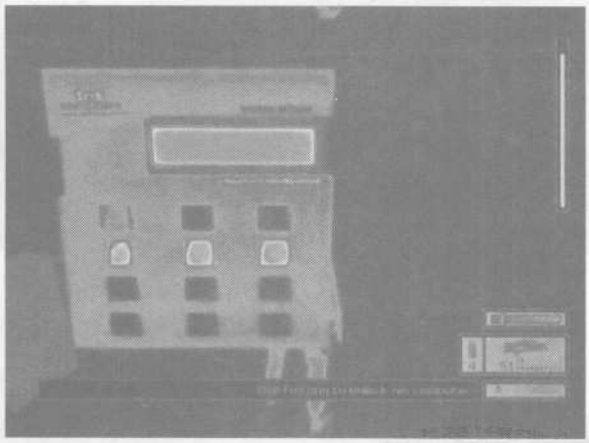
单锁（如下图所示）的口碑并不好。



著名的安全研究员 Michal Zalewski 利用高科技手段攻击测试锁的安全性，他研究的成果很值得关注。在他的论文《热成像攻击保险箱》（http://lcamtuf.coredump.cx/tsafe）一文中，Michal 发现，使用者留在号码键上的手指余温，在几分钟内都可以被热成像设备探测到。如下图。



像细胞分裂（Splinter Cell）这样的热门游戏也已经加入了这种情节。下图是游戏中的一个画面，Sam Fisher 戴着利用热成像技术制成的眼镜观察警卫留在号码锁上的痕迹。



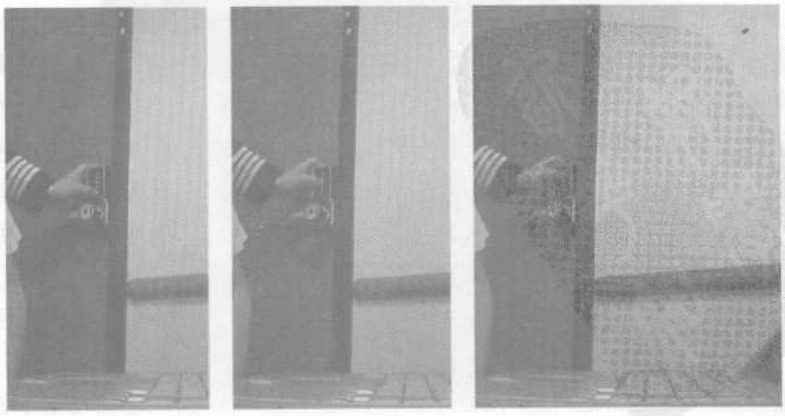
我觉得 Michal 研究得到的事实比游戏的虚拟情节酷多了，可热成像绝对是种高科技攻击手法。但本书是关于非技术的，所以让我们看看有什么非技术的手段吧。既然使用频率较高的号码键上会留下使用者的痕迹，可以用婴儿爽身粉撒在控制面板上，再将其吹去，留下的就是号码锁的密码键。或者，可以欺骗知道密码的人去触摸一些反射紫外线的荧光物质，在他（她）使用号码锁后，用紫外线灯照射控制面板，反光的键即是号码键，有点像电影《国家宝藏》（*National Treasure*）里的情景吧。如果有很强的眼手协调能力，甚至可以立即展开蛮力攻击。

但我目前所讨论的这些技术还并非真正的非技术方法。这些攻击手法需要实

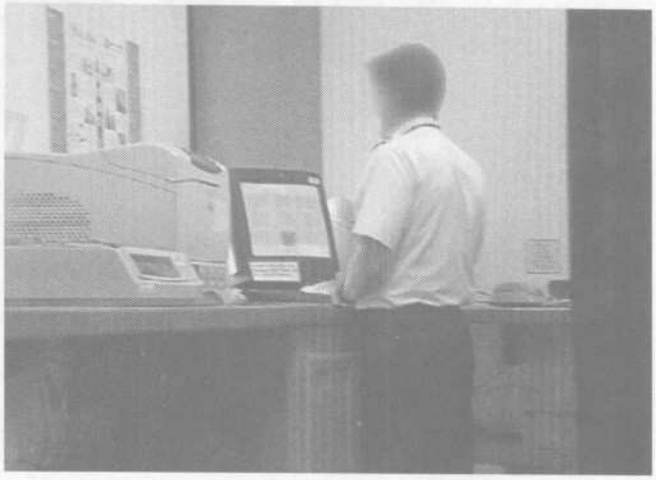
实在在的工具和一些设备，至少有些婴儿爽身粉吧。我们看看现实世界中的非技术攻击吧。跟我到机场来，这里有最苛刻和最先进的安全系统，用眼睛或相机去搜寻背后偷窥的机会。

走过安检站，我注意到几把单锁，但它们形态各异，都像是用来锁壁橱的。最后，我发现了一把单锁，好像是办公室门上的。这扇门紧挨着检验区的门，并且当我走近时一个飞行员来到门边，输入密码后推门进去了。我看到一个有窗户的办公室，可以俯视机场跑道，以及一个计算机显示屏。我发现是这种锁在保护该办公室，但遗憾的是我没有注意观察号码锁。我想找个不错的位置坐下，等下一个飞行员过来以刺探密码。离门比较近的位置比较理想，角度也很不错，我可以清楚看到他们的操作。我正准备坐下，看到了下图中的警示标语。

我装作没看到，然后坐在“禁区”里，拿出我的笔记本计算机，把相机放在键盘上，确保不被路过的人看到，就开始等待。没过多久，一个飞行员走来，手放在号码锁上。下面几张照片是当时的情景。



尽管照片的排列是随机的（或许删掉了一两个），但图中的信息是很清晰的，这说明背后偷窥很有用，尤其是在没有带热成像装置的时候。飞行员推门进去，门依然敞开。我拿起相机继续拍摄。

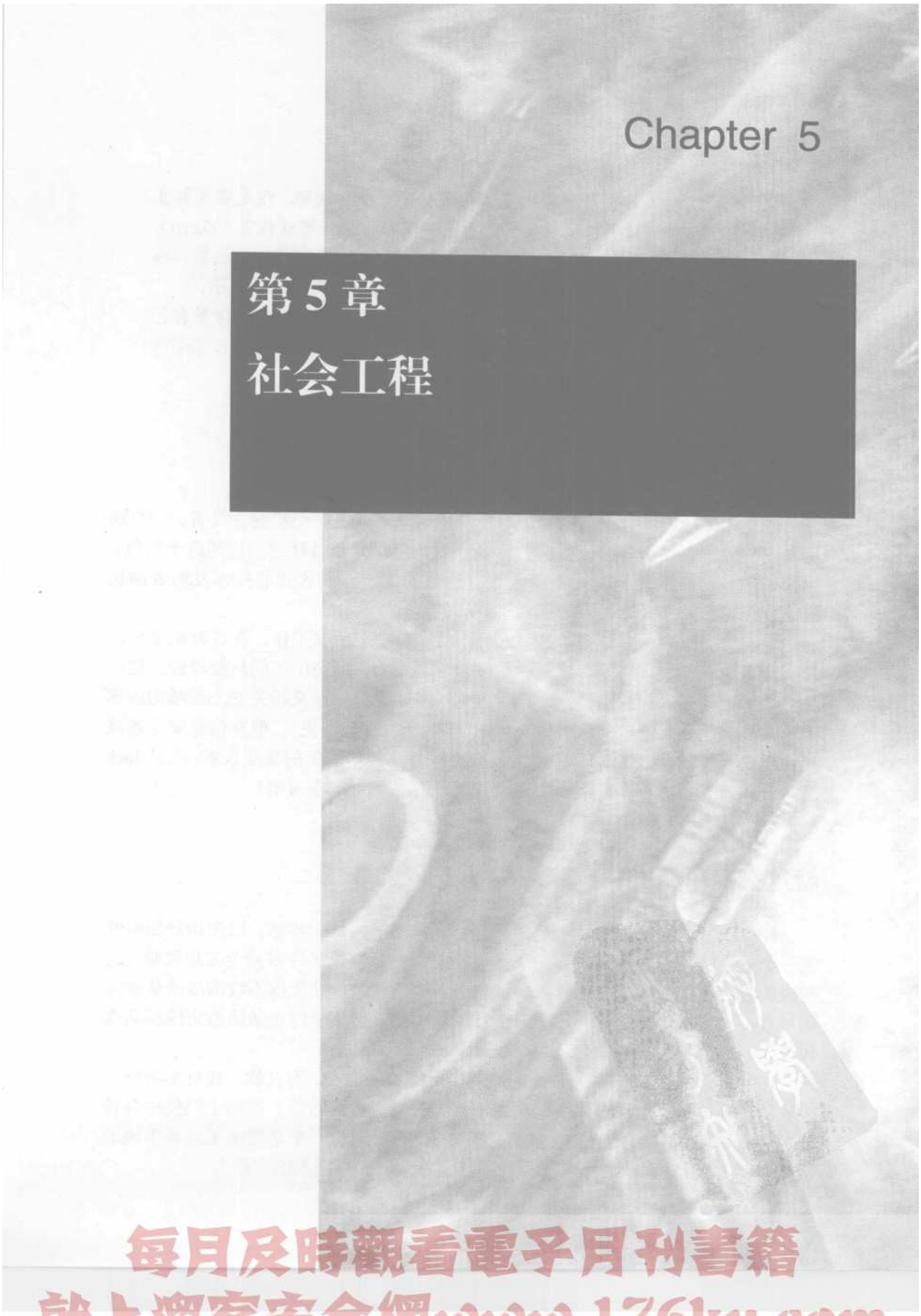


为了保护无关人员，我已经将照片模糊处理过了，但即使如此应该能看到我看到的情景。这样你会明白本书教的东西。我知道你没有在图片里看到什么有用的东西，但至少应该能够观察到5项内容，作为一名非技术黑客应该关注的5项内容，并获取更多的信息。你知道是哪些内容吗？试试看，继续阅读之前尝试一下吧。

你该怎样做呢？注意观察显示器。我们已经讲过如何在背后偷窥显示器。显示器上的粘的标签——一个小的、一个很大的。一个可能是条形码，另一个上面记录的可能是别的什么东西。再深入想想显示器是什么牌子？结合条形码，可能会得到一条线索，是谁在提供技术支持。采用社会工程方法，怎么做呢？维修激光打印机如何？另一个纸条上列着打印机的说明、IP地址、打印队列和相关信息。打印机的牌子可能给另外的启示：可以扮成打印机维修员或其他员工。你看见那台很旧的，都掉色的点阵打印机了吗？上面粘了不只一个字条。仔细看看电话上的标签。它可能包含什么重要的信息吗？注意到海报没？它是否包含对社会工程有用的行业暗语？操作终端的飞行员视野比较广，但即使如此我们也可以在办公室外轻易地做到。他是已婚还是单身？现役还是平民？喜欢整齐的办公室还是凌乱的？类似的判断会更多。

下图总结了这次成功的攻击，我不仅拍到了一个房间的潜在信息，还拍到了一个飞行员的挂绳和一串徽章。一张照片中就有这么多攻击方法可供选择。

这里重点不是如何破坏机场的安全系统、捉弄粗心大意的飞行员或者羞辱交通安全管理部门，而是要强调，在这样一个安全等级之高的环境里，非技术黑客竟能找到这么多漏洞。在这么短的时间里，如果在机场都可以搜集到这些信息，那么在其他任何地方也可以做到。



Chapter 5

第5章 社会工程

社会工程是非技术黑客武器库中最必不可少的武器，但是在实际生活中，我们对精通于这项技术的人确又爱又恨。我们喜欢佐罗（Zorro）、超人克拉克·肯特（Clark Kent）等；但讨厌 Robert Hanssen（电影《叛国者》中的主角）、Aldrich Ames（美国著名间谍）或其他的骗子。

不管你怎么看社会工程师，至少应该调整心态，学会怎样保护自己及身边的人，因为社会工程师有一个巨大的优势：在你以为这只是个游戏的时候，已经被他耍了。

引言

现在你可能已经注意到，一个非技术黑客几乎就是一个机会主义者、一名演员、一个骗子。安全专家能扮演各种各样的角色，尤其是社会工程师这个角色。黑客试用一些技术看他能否获得什么有价值的东西，而这并非技术发明者的初衷。社会工程师在人际关系方面做了同样的工作。

本章第一部分的作者是 Jack Wiles。他专职安全研究工作，在计算机安全、预防网络犯罪、灾难恢复，以及物理安全领域，有超过 30 年的从业经验。他已经培训了上千名联邦探员、公司律师、CEO 和计算机犯罪及相关安全领域的内部审计人员。他令人难忘的演讲包含了 30 年的个人“战斗史”，他在信息安全领域和物理安全领域奋战了 30 年。因为社会工程是非技术入侵的核心技术，而且 Jack 是这方面的专家，那么，下面大家就跟随他开始本章的学习吧！

就这么简单?

作为一个内部渗透测试小组的领导，我需要了解每个步骤，以便指导如何开展一个成功的内部渗透测试。正是多年的工作使我获得了许多社会工程经验。这些经验最终帮助我脱去了“垃圾箱潜伏者”的帽子，帮助我以不败的战绩从老虎队（Tiger Team）光荣退役。尽管我有多种角色，但从未停止做防盗窃或反间谍代理人，尽管那些是我的角色——准确的说那就是我。

1988 年，我成为一家大公司的内部安全小组的成员。有几次，我有幸听到一些人的对话，是“黑帽子”小组利用电话攻击受害者的对话。黑帽子们使用各种社会工程技巧获取私人信息（包括密码）。我所听到的一个老黑帽子对新手说的话在今天看来仍然是对的：“社会工程是侵入系统的最简单的方法”。

为什么攻击者偏爱利用社会工程作为攻击的首选方法呢？假如你是一名黑帽子精英，一个国际大公司想要侵入主要竞争对手的网络，如果能帮他们做到，会得到一大笔钱。简而言之，他们需要一个或更多的对手的用户的名字和密码。

假设目标公司为 Acronym。作为一个攻击者，想要知道目标网络中用户的名字没有什么挑战性。多数大企业分配用户名是系统自动完成的，取自员工的姓名。如果 Joe. Doaks 在 Acronym 工作，他的用户名就可能是 joedoaks、jdoaks、JDoaks@Acronym 或其他一些写法。如果你知道员工的姓名，可以确定他的用户名。一个最直接的方法是得到公司的通讯录之类的东西。既然你是一个聪明且业务精干的高科技黑客，可以搜索到 Acronym 的网页，找些名字出来。可以从管理人员、公关人员、技术支持里选择，随处可见的电子邮件地址暗示着用户名可能的组成。很好，剩下的就是密码了。

我准备比较高技术黑客和非技术黑客获得密码的差异。准备好了吧？下面是高技术黑客的步骤：

- **扫描 Acronym 网络，监听网络端口** 可以花些时间扫描所有的 65 000 个端口，但 Acronym 网络的入侵检测系统会发出警报。如果那样就聪明过头了，应该在隐藏模式下缓慢扫描，每隔几秒钟扫描一个端口，理想情况是将网络内的所有 IP 地址都扫描一遍。
- **安装恶意软件** 假设端口扫描成功，表明某个端口是开放的，就可以在 Acronym 网络上设置木马程序。你也可以编个小脚本，用来检测最新的漏洞，希望 Acronym 还没有在每个应用程序上打补丁。你要花费大量的精力去检测 Internet Explorer, QuickTime, Win Amp 等应用程序的漏洞，正如你挣得人生的第一桶金一样困难。但既然你想做这样的“黑客”，我们保证你可以成功将代码植入目标网络的计算机中。
- **获得目标网络拓扑图** 恭喜你！你已经进入 Acronym 的网络。它有多大？有多少子网？使用路由器还是集线器？相互怎样连接？能否找到存储密码文件的服务器？必须认真画出网络拓扑图，而且不要暴露行动。在今天这样的网络环境中，你还得防着其他黑客，至少把进入的机器的安全漏洞打上补丁，以免受到一些初级黑客的骚扰。
- **找到并拷贝密码文件** 假设 Acronym 网络服务器上运行的是 Windows 操作系统。你可能会使用 pwdump 这种工具去拷贝一份他们密码的哈希数，并传到私人网络，再尝试以文字形式显示出所有的密码。你必须从一个目标网络主机转移到另一个，像踩着一串石头过河，逐渐走近核心的密码服务器。当然，行动不能暴露，修改日志记录和注册表键值，这样某些文件就不会更新它们被访问的日期。

- **运行破解工具破解加密密码文件** 获得了密码的哈希数，行动也没暴露，下面你就要将字典文件以及一个巨大的（rainbow table）加载到 John and Ripper（破解工具）中。不到 1h，就可能得到一些密码（如果想在实验条件下看到这个过程，可以观看 Security Wise 的视频，《密码是怎样被破解的》，http://video.google.com/videoplay?docid=4683570944129697667）。

结果出来了，现在可以长舒一口气了，仅仅花了一周时间。

再看看非技术黑客怎么做。准备好了吧？分如下几步：

- 打个电话
- 再打个电话：聊天——获得信息——合法登录

电话铃响了，下面我会说明怎么做。现在，通过对这两个流程进行对比你就会发现社会工程比高技术攻击要简单的原因。

这两个步骤组成一个攻击模式，但这个模式是有难度的。有时，社会工程的方法能让你轻松得到想要的东西。一天，我站在西雅图的的大街上等公交车，身边的两个人在讨论他们公司的网络。其中一个向另一个描述自己既时髦又酷的口令，就在这样公共的场合。他觉得这没什么不安全的，别人又不知道他是谁。我从后面悄悄看了一眼这个在大街上谈论自己口令的狂妄家伙，发现他的工作证就挂在他裤兜旁，上面写着他的名字，上方是 Amazon 公司的 logo，而这家公司的总部距此也就只有两栋楼。太让人吃惊了。

社会工程就这样简单，而且社会工程不依靠任何高科技设备来发动攻击，只是用技巧攻击对手的心理。大多数情况下，用文件夹或廉价的商业卡片就可以完成。社会工程不仅操作简单，而且成本非常低。

在过去的 15 年里，我领导过几个内部渗透小组，受雇于一些想测试自己大楼安全系统的客户，我明白作为一名成功的反面角色是多么的容易。我们假扮成他们的员工入侵大楼，没有一次失败。每个碰到我们的人都以为是他们的同事。

这怎么可能呢？怎么不可能，这就是人的本性使然。

人的本性与弱点

这不是第一本介绍社会工程的书。关于这个主题的书读得越多，对其中的共性了解得越透彻。一个社会工程师利用我们有同情心和乐于助人的本性来对付我们，来了解我们的工作。

有关这方面最好的著作出自 Kevin Mitnick，他被誉为社会工程之王。他的著作《欺骗的艺术：控制安全系统中的人》（The Art of Deception: Controlling the

Human Element of Security）通过一个个的小故事挖掘出人类善良的本性。

Mitnick 一般在别人有困难且能够解决的时候才提供帮助，当然，通过简单交谈就能得到想要的信息。通常他询问的信息不是敏感信息。例如，如果你在一家国有银行工作，有人打电话询问另一个支行的地址，这种信息看起来并不是什么要保密的。所以支行的人给予了回答。在这次通话中，他们无意的泄露了很多信息：只在内部使用的行话、表单的官方称呼、账户号码位数。

Mitnick 非常善于将这些只言片语组合起来以获得更多信息。如果某人给你打电话用的都是业内行话，好像对你们的业务很熟悉，并且对管理和客户的体验和你一样的话，你会认为对方是自己人，而不是外人。通常人们都乐意帮助自己人。

我当然不反对乐于助人，但应该时时与谨慎相伴。对于这些内容，我们通常考虑员工以外人员的威胁，就是不属于大楼内的人的威胁。这种陌生人应该不难看到，并且很容易阻止，对不对？

你好，进展如何？

“那些陌生人，不在大楼里的工作人员”就是我的内部渗透小组将要扮演的角色。当我们混入大楼而没有引起注意，我们很明显不属于那里（不是通过应聘进入那里，但没有一个雇员知道）。可能间谍或未来的恐怖袭击者也会采取这种方法混进去查看情况。理论上，楼内的一些员工应该能发现有“木马”的存在。无论周围的安全情况如何，只要控制入口，应该能够抓住非法进入者，但我们从未碰到这种情况。

这些年，我们被雇是期待被抓住，证明系统安全。我们的攻击方法越来越多，小组在大楼里待的时间也越来越长。每次任务结束，我们就像公司的员工一样大大方方走出来，心里当然在希望被人抓住，但从来没有！那些员工，总是轻信我们的话。

善良和乐于助人的含义是一样的，但做个傻瓜却完全不是那么回事了。到现在已经超过 30 年了，我发现大家对这方面缺乏清醒地认识。这些年来，社会上很少有文章去揭露这种秘密的、可以被阻止的攻击。

我们是好人，但我怀疑有许多坏家伙会比我们更熟练地使用这些方法，他们同样不会被抓住。并且我们工作在自己制定的一些原则之下，但是那些坏家伙是不会考虑原则的。采取暴力进入，利用撬棍通过门窗，是我们所不屑的。冷静的头脑和社会工程技巧是我们的主要工具。因此，如果没有侦察到我们，尽管工作在自己制定的规则之下，想象自己对凶狠攻击者来说是个多么诱人的目标，而他要做的就是赌一把：发财或者入狱。

需要提高防护意识。最后，我告诉你是怎样诱使员工透露出机密信息的。这样可以帮助增强防御意识。

受害人的思维

我们每个人，在任何时候，都很可能成为某种社会工程攻击的对象。完全没有这种风险是不可能的。但我们应该做些事情尽量减少这种风险，下面的内容我会给大家讲解怎么来做。

如果没有某种形式的培训（实践），学习如何抵制社会工程人员，你会很容易成为受害者，甚至不知道它的存在。

人们通常以信任和可预测的方式思维，而这意味着背离正常情况的事情的发生对我们而言是不可能的。他们没有时间进行深思熟虑，以及该作出怎样的反应。社会工程师就是靠这个实现攻击的。人们一般察觉不出什么问题，也不会明白自己怎么就被糊弄了。总之，人们一般很难对社会工程做出有效的防范。

“社会工程永远不可能攻击我们公司！”

上面的话是我朋友的原话。当时我们在讨论系统的整体安全和社会工程的威胁。我告诉她自己的经历，但朋友觉得我的这些伎俩对她的公司无计可施，因为她认为公司的安全措施很过硬。“我们有很棒的安全措施，并且我的员工也不会向任何打来电话的人透露任何信息。”她自信满满。

“给我 90 天，这样你不会知道我会什么时候打电话，让我来检验一下。”我说。

她同意了，但有个条件。如果攻击成功，她要我用录音带记录下来通话内容，以便给她的员工培训用。我喜欢这个主意。比赛开始了。

几周之后，我打了电话。

“下午好，”很友好的声音，“医疗集团，我是玛丽，有什么能帮你吗？”

我马上用医生的口气回答，“你好，我是 Wiles 医生”（这样讲话很有趣，因为全是假的），“我想让你帮个忙。我们有个项目和你们在 Richmond 的类似，并且打算购买新的医疗计费系统。你们使用的是完全自动的计费系统吗？如果是，使用效果怎么样？”我友善的话语没有引起对方的任何怀疑。这个问题很显然没有任何值得质疑的地方。

“是的，我们使用自动计费系统，”她答道，“我们把它叫作医生数据库系统（Doctors Database），在科罗拉多州的丹佛市。”

至此，感觉还不错。她好像愿意多说点，我就多问了几个问题。“你们碰到问题的时候他们提供帮助吗？我听朋友说付款之后他们就不管了。”

“提供，我们对他们的服务很满意。”玛丽回答说。

“系统升级和维护呢？他们有专人来做吗？”

“没有，他们通过一个系统附带的调制解调器来解决问题，我们还没有碰到过需要他们上门维修的故障。”

我继续提问。“在做决定前，我想和维护医生数据库系统的人聊聊，确认这个系统是我们需要的。你能给我技术人员的姓名和电话吗？你知道，有些技术人员的话很难理解，我总觉得和他们交流会好点，这样以后我们的管理员如果遇到什么技术上的问题也方便和他们交流来解决问题。”

玛丽显然对医生数据库系统很熟悉，因为很乐意告诉我。“好吧，我们和 Jerry Johnson 联系，他很随和。你可以东部时间 6 点之前打电话，他下午应该在办公室。电话是 800-555-1212，24 小时都有人服务。”

她不会知道我已经得到了需要的一切。再多一个问题，我就可以很礼貌的对她说谢谢、再见了。“耽误你太多时间了，非常感谢。我们买了付费系统之后，如果我们的管理员有什么使用的问题，我们能打电话给你们的数据库管理员吗？你知道，咨询正在使用系统的人总比让卖家来回答简单得多。我保证不会再麻烦你了。”

她说她就是数据库管理员，也很乐意帮助我们。我顿时觉得生活充满了阳光，能生活在南方温暖的阳光下真是太棒了。

“谢谢你帮了我这么大的忙，”我礼貌地说，“除非遇到管理员确实解决不了的问题，否则我不会让他们和你联系。祝你周末愉快，再次感谢你。”

我从玛丽那里得到了什么呢？

这次看似平淡的通话让我获得了攻击需要的一切信息。下面就是我得到的：

- 她叫玛丽，是卫生部门的数据库管理员
- 医药付费系统称为医生数据库系统，公司位于科罗拉多的丹佛市
- 在丹佛市为他们提供技术支持的人叫 Jerry Johnson
- Jerry 通过调制解调器访问他们的计算机进行技术维护

一般说来，这些并不是什么敏感信息，大多数人都会乐意告诉你。注意，我并没有问关于计算机的问题，当然也就没问任何关于登录 ID、用户名或密码或问题。

最后一击

两周后，周五下班前的几分钟，医疗集团的电话响起。

John 在电话响了三声后才接起，有点不耐烦，他知道这么晚带来的电话会占

用他宝贵的周末时间。

“下午好，医疗集团，我是 John。能为你做什么吗？”

我用拿手的社会工程的音调开始了攻击。“你好，John，我是 Bill Jenkins，是丹佛医生数据库系统总部的。我们电话通知所有的客户，医疗付费系统有个严重的问题。好像是我们最后一次更新时染上了病毒，直到下午才发现。它可以破坏所有的账目记录。全部的技术支持小组都在电话通知我们的客户，让他们尽快知道发生的问题。我知道玛丽平时与 Jerry Johnson 一起工作，但她此刻在为别的客户服务，所以让我来维护你们的系统。我能与玛丽通话吗？”

对方暂时没有回答。我可以感受到 John 在为浪费了周末的第一个晚上而气得发抖。他最后回答“周末放假，玛丽今天休假。我替她备份数据库，我可以帮你。”

事情有眉目了！我开始设置陷阱。“玛丽不在啊？”我努力让语气听起来有点慌张。“John，我必须登录到系统内才能开始维护，而我现在没有 Jerry 的登录信息——你知道，用你们的 Modem 登录需要输入号码，用户名和密码。如果不能从玛丽那里得到这些，那将会很麻烦。事情很紧急，需要马上动手，病毒可能在整个周末都难以控制。”接着我就闭嘴了，让安静来说服他。

我做到了。我能听到他在翻文件的声音。“我在她笔记本上找到了。电话是 555-867-5309，用户名是 doctor，密码也是 doctor。”

我再回到拿手的路线上，让他完全失去戒备。“John，你帮了我大忙了，我可以使用了。但清理工作需要大约四个小时，我知道已经周五下午了。我不愿浪费你的周末，我会把补丁安装上，在你周二回来时一切都会正常。再次感谢你的帮助。周末愉快！”

John 挂了电话后轻松了许多，此刻他能记起的可能只有 Bill Jenkins。你知道，除非他的老板以后放磁带给他听。

这种诡计为什么能够成功？

没有任何警觉性训练，没有任何的怀疑，在电话里与陌生人交谈时，任何人都可能遭到这种攻击。

许多听了这两段攻击录音的人告诉我他们以前好像也有类似的经历。第一个看似平淡的电话为第二个让人信服的电话做了很好的铺垫。从周五下午到周二早晨，计算机里可能已经发生了很多事情。真正的医生数据库系统公司知道这件事吗？绝对不知道！他们无从知道一个黑客在打着自己的旗号行骗。Jerry Johnson 真的是医生数据库系统公司的技术人员吗？绝对是！玛丽经常和他一起工作。但 Bill Jenkins 是我捏造的名字，是我设置的一个令人信服的场景，并糅合进去一些真实的因素。

撇开这次攻击而言，该公司的数据库系统的密码设计的太不安全了。我不会像密码爱好者一样用词典里的若干词汇设计密码，另外这个话题也不是本书要讨论的。如果你对密码有兴趣的话，可以看看 Mark Burnett 的《完美口令》一书（本书已由科学出版社引进出版）。

应对社会工程攻击

提高警惕是应对社会工程攻击最好的防御方法。应该教育每名员工社会工程攻击发生的可能性，而且危害很大，提供一些简单的防范方法。下面，我们关注对付社会工程攻击应该注意哪些重要内容。

主动提问

如果有一件事情是我在小时候学会，那就是永远不要畏惧提问。你不知道答案，就问，提问才显示你的才能。自己觉得什么都懂而不问才是蠢材。即使你知道答案，提出问题，可以机智地考察别人对于问题的看法。人们喜欢利用假设来思考问题。我认为你打电话来问我，那你对这个问题肯定有些了解，否则为什么要打电话？

面部表情和肢体动作也是人们交流的方式，但在电话里却不起什么作用。通过反问可疑的来电者，大多数人会因为你的警惕而打消攻击的念头。索要电话号码，这样可以打给来电者。虽然这样做起不到保护作用，但我常会让潜在的社会工程攻击者在这个问题之后挂电话。因为他们还没有不能被追踪的电话号码。

积极做好应对，并形成书面策略，告知员工，打电话的时候，若有人提问到关于公司的问题，哪些可以回答，哪些不可以回答都要写清楚。每月的例会上，可以把这方面的问题提出来，可以称为“社会工程攻击演练”。尽管我从不喜欢演戏，但在这个领域我的角色却很有趣。来电者可能涉及工业侦探、间谍、蓄意破坏者、好奇者等。如果公司的“防御”小组将电话里可能提问的问题事先整理好，很可能真正的社会工程攻击者的问题就在其中。在角色扮演的场景里打电话的时候，要仔细审查，认真考虑再做回答。

一旦员工意识到这种威胁的存在，一旦有一点觉得奇怪，他们在接电话的时候就会很小心谨慎。应对电话攻击的效果就会有很大的改善。当然，接电话的时候不应该太粗鲁或用言语侮辱他人，在礼貌礼节的前提下保持镇定和警惕。如果来电者是正常的人员，他们会体谅你保护公司信息的良苦用心。在用信用卡购物的时候，出纳员会礼貌地请你出示身份证，你不觉得这样比较安全吗？

安全意识训练

令我吃惊的是，员工对提高公司的安全防护很感兴趣。但也不奇怪：公司做好了，他们也有利了，至少，可以保证工资按时发放。

在我们开展安全意识的培训项目后，参加培训的人都很积极。他们会发给我一些这方面的文章。令人欣喜的是，现在，我的学生也变成了老师，而最终的结果是每个人都获得了巨大的回报。随着越来越多的人参与，安全问题会变成很有趣的挑战而不是令人不快的琐碎工作。

海报

做安全问题研究的时候，我做了很多关于如何提高安全意识的海报。用海报这种方式宣传很好，我希望用最少的钱达到最好的宣传效果，也符合我方便在复印机中复制的标准。在头脑中有了这些想法，我坐下来看一本艺术书并通过一点自由的想象。两个小时就画了很多的画，并增加了许多睿智的描述短句。针对特定的群体，我每 3 个月就会寄出一份海报。没多久，很多人打来电话想要订阅我做的海报，而且有人开始收集这些海报，并把它们进行展览。

创作海报容易，但内容必须准确，否则就失去意义了。记住，大多数的雇员不是 IT 领域的，他们不知道我们的行话，以及缩写是什么意思。最后需要注意是，你的内容一定要有煽动性，不要让目标人群觉得无关紧要、很虚幻，甚至厌烦。你知道："SB1386:是法律条款！"如果你不是 IT 人员（并且不在加利福尼亚），不会明白海报是在提醒时刻注意州法律的规定公司要保护客户的隐私。

如何才能让安全问题的海报吸引人，让人难忘呢？下面是我的建议：

- 使用通俗的语言，不要使用缩写词或专业术语。不然非 IT 人士看不懂。
- 一张海报一个思想。不要在一张海报上列举 5 条、10 条，甚至 20 条警示标语，那样人们根本记不住。别想一劳永逸，如果还有什么要说的，就再做一张海报。始终要一张海报表达一个思想。理想的情况是，海报简单明了，不超过 15 个单词。
- 表达要幽默。安全问题无儿戏，但如果让员工印象深刻，幽默比强制的效果好得多。
- 形象为基础，关注流行文化。海报可以加勒比海盗、史莱克等角色为基础制作，这样才能让人印象深刻。必须具备的能力包括想象力、一点 Photoshop 技巧，以及对安全问题的关注（包括怎样避免侵权）。

- 如果建议人们怎样做，就着重表达出来。也许可以在海报中设计个懒人的形象，并加上这样的注释“记住，黑客想要你的密码！”但是员工应该这样做呢？较好的是：“越长越好！密码至少要14位！”
- 使用海报作为辅助手段。即使做出世界上最好的提高安全意识的海报，仅靠一张海报去提高员工意识，是远远不够的。员工必须接受了更深层次的安全培训，再利用海报提醒他们，才会收到良好的效果。

如果你想做一些大众型的海报，但没有什么好的构思，可以到网上找资料。可以访问 Gary Hinson 的网站 www.noticebored.com 或者 http://www.ussecurityawareness.org/highres/security-awareness.html参考一些以前的例子。

将这些海报发出去后，大约过了6个月，我迎来了一位素不相识的客人。他走近我的办公室，打过招呼之后，说自己是公司在外的审计员，一直在我们的大楼里做审计工作。我和公司的那些审计员比较熟悉，但这位却是我见过的第一个所谓的外部审计员。握手的瞬间我有种感觉，像在小学时被叫到校长办公室，心里不禁问道：我做错什么了吗？我不在乎自己有这种感觉。但当他告诉我想见见制做这些海报的人时，我才放松下来。它们看似简单却含义深刻，他想回到公司后也这样做。我表达了谢意，并同意他的想法（外部审计员得到他想要的，不是吗？）。这件事我让我印象深刻。对于一个审计员来说，他们总认可一件事：勤奋。

后来，我甚至发起了一项有奖竞赛，鼓励大家提出有创意的想法，用来改善明年的海报设计。我准备好了奖金和其他一切事情，只需一点想象力就能创作自己的海报，享受创作的乐趣吧！

视频

随着提高内部安全意识研讨会的需求逐渐增多，有很多问题需要解决。越来越多的组织想要我们的报告内容，当然我不可能给他们一一寄去。我下一步计划是准备一些视频资料，提供他们使用。这样做花费可能很高。一个影音质量不错的碟片每做一分钟就需要大约1000美元。这么高的价格，即使一个30min的视频，也会大大超出大多数组织的支付能力。

我脑子里有个不太完善的想法。通过朋友的帮助，再加上一个摄影机，我用近2h的时间制作出的视频基本上是零花费。足足30min的视频，可以展示给一个小组的成员观看。接着我又做了一段照片的视频。之后的工作是将两段合成一段。我们试了几次最后成功了，终于找到了便宜又高效的方法。我们不知道这第一次的尝试会有怎样的结果。我们做了100份拷贝，分发到公司的各个部门，可喜的是拷贝都放映了很多遍，以保证每个员工都有机会看到这个视频。据我所知，直到现在这段视频仍然在放映。

视频制作工具

你也许在寻找能帮助制作安全培训视频的软件。Techsmith 公司的基于 Windows 平台的 Camtasia 是不错的选择（www.techsmith.com）。它能记录你计算机屏幕上的所有操作，是一个视频屏幕捕捉工具，再加上声音记录；这绝对是个完美的方法。苹果平台的用户可以考虑使用 Ambrosia Software 公司的 Snapz Pro X（ww.ambrosiasw.com）。两个工具都能记录屏幕上的视频、文本和实时的音频。如果有苹果笔记本，可以使用内置的摄像头来记录播放的视频，使用 iMovie 处理你的视频，这样制作视频就不需要再买摄像机了。

我和大家分享这些是为了告诉大家，如果我能做到，你们也一样可以做到。我觉得自制的视频资料相当流行。它们没有繁多的商业广告，而且画面都是真实的场景，观众很容易认可。虽然制作工具越来越复杂，但价格越来越低。如果你亲自尝试，相信结果会让你大吃一惊。

举个例子，某个 IT 部门出于公益的目的，制作了一些很好的提高安全意识的视频，下面是来自 WatchGuard Technology's LiveSecurity 小组的作品：

Drive-by Download

http://video.google.com/videoplay?docid=-3351512772400238297&q=livesecurity

Contrary Wisdom from Syngress Authors

看来制作费用很高，可事实并非如此。拍摄地点选在了一家旅馆的客房，工具只是两盏台灯、一个相机及一支黑色的鹅毛。

http://video.google.com/videoplay?docid=-2328105253826896657

如果喜欢这种类型的视频，可以在www.video.google.com上搜索 WatchGuard LiveSecurity 就能找到更多视频。

如果你是美国公民，也可以从国防部免费获得信息安全培训视频。很多是针对非技术人员的。想获得更多信息，还可以访问http://iase.disa.mil/eta/iaetafaq.html。

证书

公司也有人对我的研讨会、海报和视频吃惊：如内部审计员和律师们。因为有了外部审计员，内部的这些家伙们认为我举的这些例子，只要经历丰富了自然就可以提高安全意识。我们的努力是为了证明公司在尽最大努力防范威胁，既包括内部也包括外部。我最终制作了“代表证”，每个参加的人都有。

证件花费不多，但做出的成品却看着很专业。实际上，在公司里转一圈，发现许多证件挂在桌子附近。可以像我这样制作公司的证件，只需一些卡片、文字编辑工具和打印机就可以。设置字体和字号，将模板做好，其他的就只需填上姓名，邮箱之类的信息了。它们和你以前见过的一样的专业，而内部审计员也会很高兴的看到它们悬挂在墙上。

来自内部的威胁

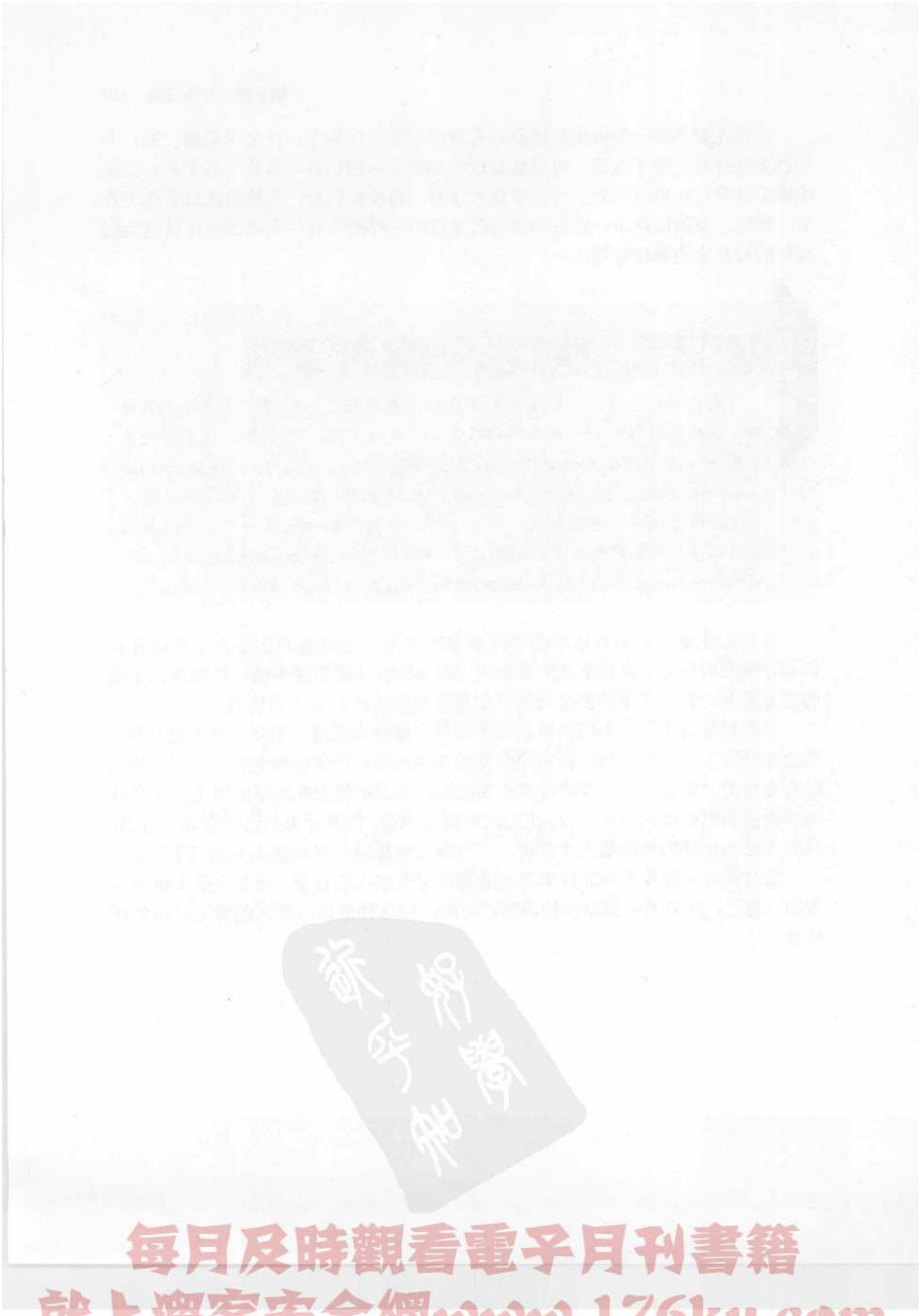
来自内部人员的威胁是无处不在的。我所知道的任何可能的安全威胁都来自公司的"内部"。这个问题很复杂，我就不在这里多说，想了解更多信息，可以浏览Eric Cole和Sandra Ring合著的*Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*这本书，这是一本非常棒的书。

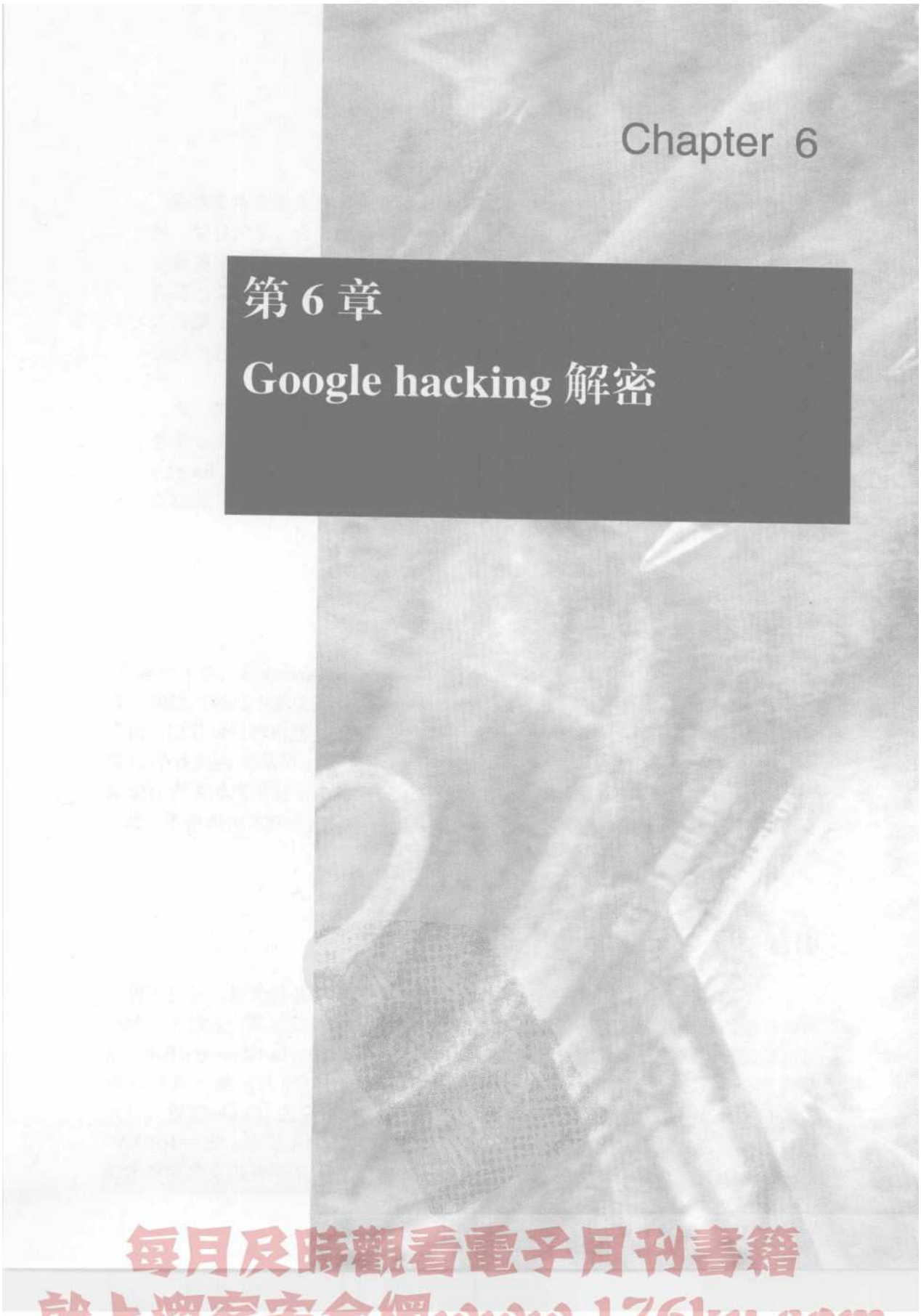
在网上搜索，也能找到一些关于什么样的性格的人倾向于做间谍或诈骗的文章。美国军方有这方面的文件，可以访问http://www.smdc.army.mil/ADR/emotion/emoteT1.htm#Behavior Patterns Associated with Espionage。

提高安全意识的教育活动需要开展多长时间？也许直到你停止工作或计算机不存在的时候吧。我并不是危言耸听，因为随着计算机越来越广泛地深入生活的方方面面，它所带来的安全问题必定越来越成为我们关注的焦点。

提高对社会工程攻击的防范意识听起来可能有点沉重。实际上并不是那样。学会质疑陌生人以及加强防范很快会变成本能反应。仔细想想生活中学到的其他的安全行为。例如，在人多的时候不要点钱；不要把包丢在旅馆的桌上；在经过哪些街区的时候要快速地穿过；出门的时候要锁门。很多行为都已经变成了习惯，只有神经不正常的极少数人才会说，"外面这么危险，我永远也不出门了"。

抵抗社会工程攻击和非技术攻击的意识会变成人的直觉，而且会越来越根深蒂固。总之，防范的关键是保持清醒，时刻注意这种危机以及遇到情况时该怎样处理。





真正的非技术黑客通过观察周围的事物就可以积累很多重要数据，但通常数据本身是没有意义的。当说到如何把数据变为信息的时候，好莱坞电影展示了黑客在黑色墙壁、红色灯光、有 32 个液晶显示器的房间里攻击北美防空联合司令部（NORAD）的计算机中心的情景。现实情况是，黑客根本不需要有自己的计算机来做这些事情。如果他能进入公共图书馆、文印店或网吧，就能利用 Google 处理数据，把它们转化成有用的信息。平时，黑客会用 Google 来搜寻敏感信息。

本章摘自我的书 *Google Hacking for Penetration Testers* 的第二卷，将介绍仅仅凭借搜索引擎和一些技巧的黑客能够做些什么。还是要提醒，这不是非技术攻击，我更愿意称它为低技术攻击。Google hacking 是每个非技术黑客武器库里必备的工具，看过本章的例子之后，你就会明白我为什么这样说。

引言的引言

本章是从我一本书（*Google Hacking for Penetration Testers*）第二卷中摘录的。作为黑客中最流行的非技术方法，Google hacking 已经成为每个黑客武器库里必备的标准武器了。我通常不喜欢摘录的东西，但最好还是把内容告诉你们，而不是仅仅指出然后让你们再去买一本书。出于这个想法，我从现在流行的有关 Google hacking（基于 Google 搜索的黑客攻击）方面的书中摘出来相关内容完成了本章。既然是摘录的内容，本章节的风格可能与本书其他章节的风格不一致，敬请谅解。

引言

一个 Google hacker 会在因特网上花很多时间去搜集各种信息。通过不停的搜索，他们希望找到真正的、最新的、有价值的东西，然后与其他人讨论，分享自己的发现。这些事情我亲身经历过。作为 Google Hacking Database (GHDB) 以及搜索引擎攻击论坛（http://johnny.ihackstuff.com）的创始人，我一直很好奇 Google hacking 能带来什么。传言是真实的——充满创造性的 Google 搜索可以帮助找到医学、金融、财产甚至是机密的信息。尽管政府颁布法令，出台 HIPAA、Sarbanes-Oxley 以及 Graham-Leach-Bliley 这样的规范，并不断发出安全警告来保

护这些涉密信息，但问题仍然存在。源源不断的资料仍充斥到因特网上，Google黑客马上就能得到它们。

为了揭示这种潜在威胁，我开始在Black Hat和Defcon这些安全会议上做相关的报告。另外，我准备出版自己的第一本书。写了几个月之后，我觉得我们做的工作最后可能会引起社会上大多数人的注意，但也可能收效甚微。但我知道肯定会有越来越多的人关注和讨论Google hacking。

Google Hacking第一版带来了变化，但却没有《Google Hacking 大揭秘》引起的波澜这么大，这是我在Google Hacking会议上讲座里有趣的一个环节。对我来说这个展示并不是很重要的一件事情——它只是由一些我亲眼所见的Google hacks的屏幕截图组成，再加上我进行的一些有趣的Google搜索，以及网络上其他人的一些搜索；我把截下的屏幕截图一一展示，并对每幅图进行评论。每次展示的时候，我都能使观众疯狂大笑，因为那些黑客仅仅用浏览器和搜索引擎来武装自己就可以造成一些荒谬可笑的结果，但人们笑过之后还是会很有启发的，很久之后他们还会讨论这些截图。这些照片中的内容就是用Google hacking做到的。这些照片集中体现了Google hacking的巨大威胁。

这就是在Google Hacking一书中摘录这些的原因。为了同这个展示的原始格式相一致，本章将着重展示那些图片而避免空谈，这是因为那些图片自己就可以进行讲解。本章中的有些截图已经过时，还有些甚至在网上已经不存在了。但这是一个好消息，这意味着在这个世界的某处，有人（或许在不经意间）不再是一个Google菜鸟，而是向更安全的态度迈进了一步。

无论如何，我使用了许多过期的照片，来很好地回忆那些紧张的网络资源的保护工作，那些图片可以证明这些威胁时很普遍的，可能在任何人身上发生，同时历史也表明确实在每人身上都发生了。

所以言归正传，好好阅读这个印刷版的《Google Hacking 揭秘》，是由我和Google hacking社区为大家带来的。

极客的工具（Geek Stuff）

这部分是关于计算机的内容，是关于技术的，也是极客们的东西。我们将看到一些Google黑客们揭露的有趣技术，它们都是真实的。先从一些设备开始学习，这些设备与网络确实无关，除非目标是帮助一个黑客。接着是了解一些开放的网络设备和公开应用程序，这些都不需要什么真正的黑客技术。

设备

任何黑客都有很多工具可供使用，但本章介绍的工具的有趣之处在于它们是在线的——它们在 Web 服务器上运行，并允许攻击者获得来自服务器的结果。更糟糕的是，这些应用驻留的服务器都有智能 Google 查询装置。我们将从手头的 PHP 脚本开始（图 6.1），它允许一个网页访问者 ping 任何一个网络上的目标主机。ping 这个功能很好用，但为什么要向匿名访问者提供此服务呢？

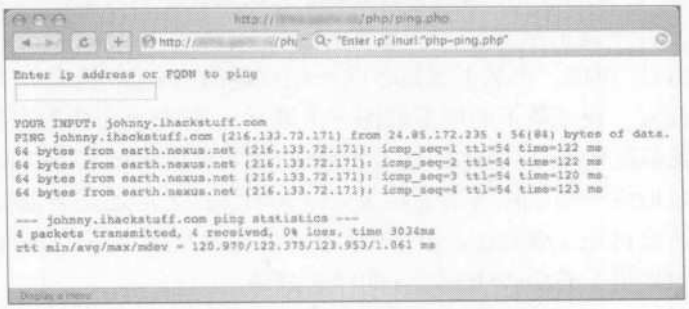


图 6.1 Php-ping.cgi 提供免费的 ping 服务

和 ping 工具不同，finger 工具已经很久没人用了。这个服务可以让攻击者查询 UNIX 主机的用户，还可以列出诸如用户连接时间、主目录名、全称等许多信息。输入 finger CGI 脚本，是一个很笨拙的让这恼人的服务网络化的尝试。如图 6.2，一个有效的 Google 查询可以定位脚本的运行位置，提供网页访问者使用 finger 服务查询远程主机上开启的服务。

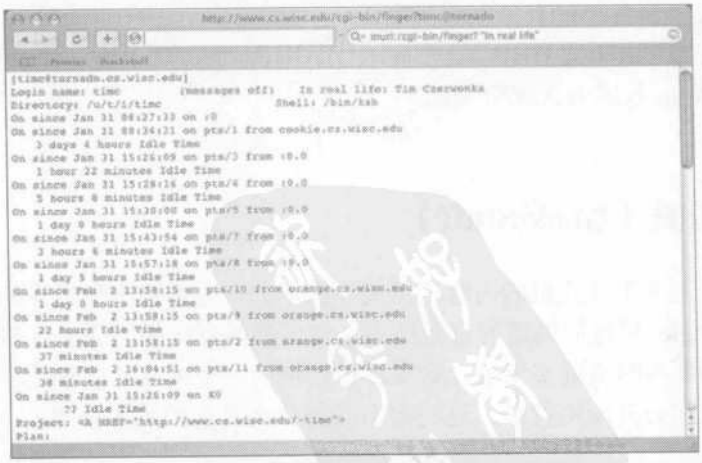


图 6.2 Finger CGI 脚本允许远程 Finger 操作

ping 和 finger 查询服务相对来说没什么危险，大部分系统管理员甚至不会在网络中注意它们。另一方面，port scans（端口扫描），则是相当危险，细心的管理员（或者一些防护软件）会记录下 port scan 的来源。尽管现在的大部分端口扫描工具提供秘密运行的功能，但一些 Google Hacking 的技术更超前一些。图 6.3（Jimmy Neutron 提供）是一个提供访问者对某个目标进行端口扫描服务的网站。

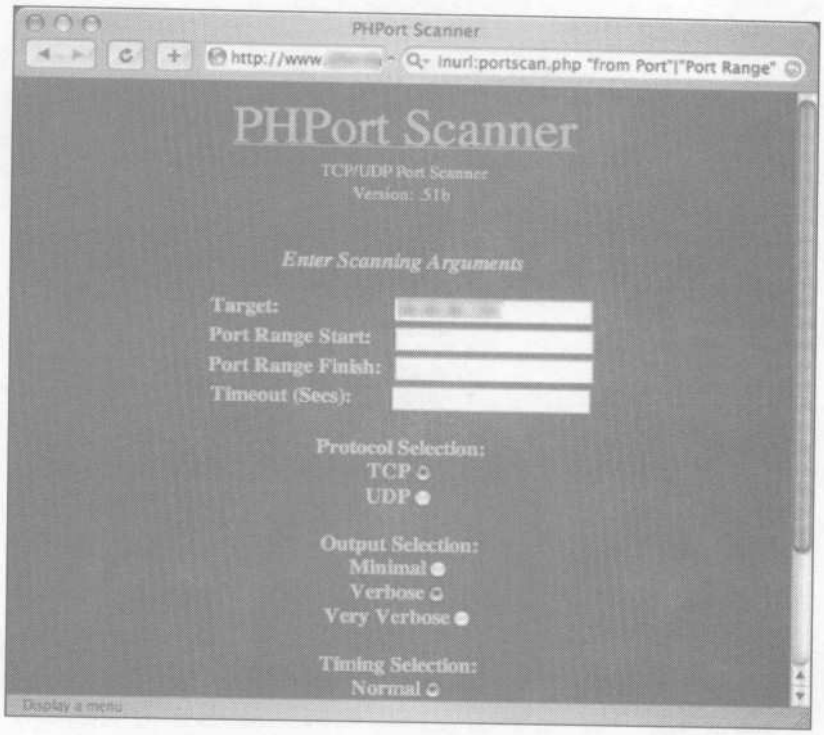


图 6.3　PHP 端口扫描器——一个优秀的基于网络的端口扫描器

记住，这种形式的扫描是来自于 Web 服务器，而不是攻击者。即使最谨慎的系统管理员要想追踪这样的扫描也要花费一番工夫。当然，大部分攻击者不只进行端口扫描。之后，他们还会利用其他一些网络设备去刺探目标，以确定他们的真实位置。然而，如果一个攻击者登录了这样的网页（图 6.4），利用远程服务器上的 Web 应用中的 Perl 脚本，就可以使用各种网络刺探工具。刺探工具又一次看起来是来自网页服务器的，并非来自黑客。

如图 6.5（由 Golfo 提供），网页上列出了一个学校的“学生注册系统”中的主机名字、IP 地址和设备信息。在界面上单击会看到更多关于网络结构的信息，以及与其相连的设备。系统在可读性高的用户界面以及 Google 搜索定位上做了很多工作，但是却很少在攻击者的刺探上做工作。

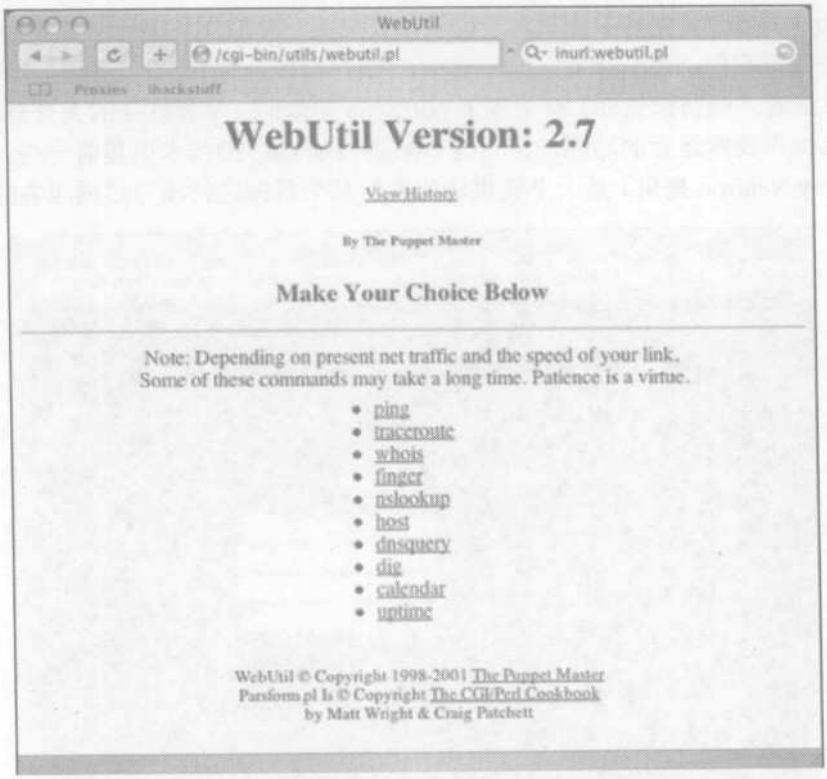


图 6.4 WebUtil 几乎可以让入侵者做任何事情

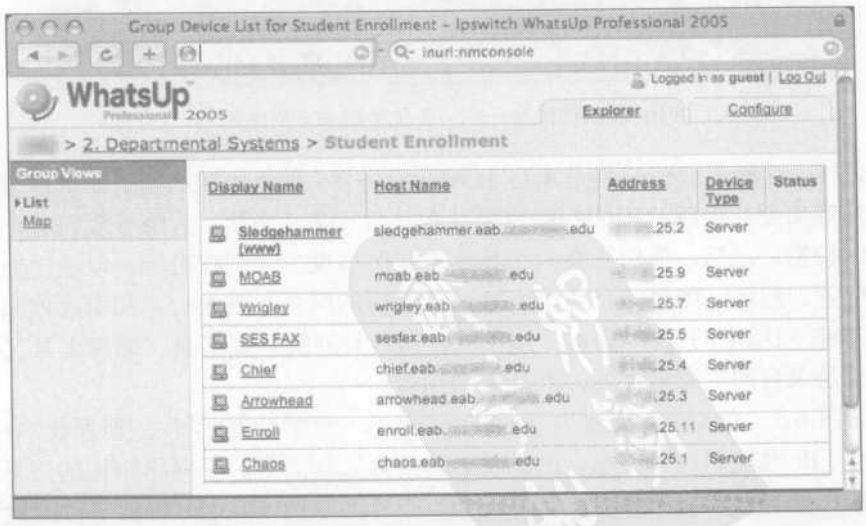


图 6.5 WhatsUp 界面向来访者提供有价值的信息

开放型网络设备

为什么入侵网络服务器或设备时，只需单击进入开放型的网络设备？还需要入侵别的网络服务器和设备吗？如图 6.6（Jimmy Neutron 提供）中的这种管理设备，经常列出各种设备的类型信息。

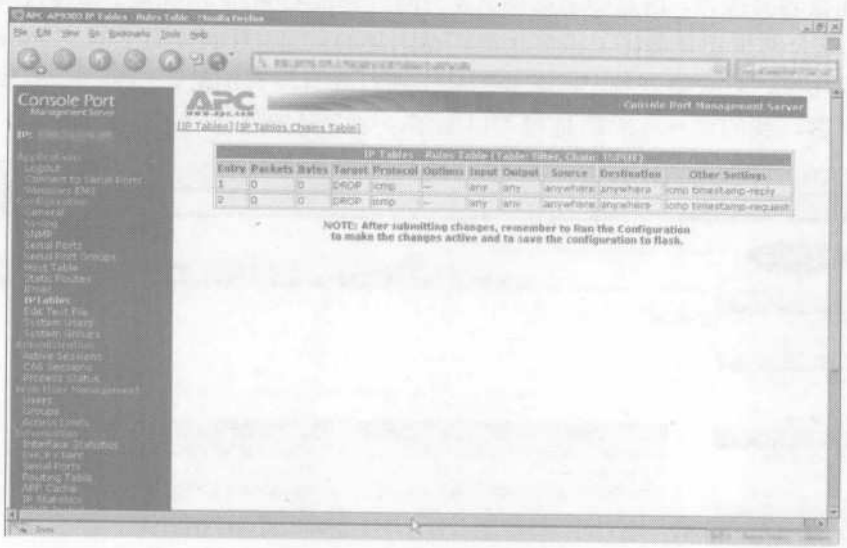


图 6.6　开放的 APC 管理设备

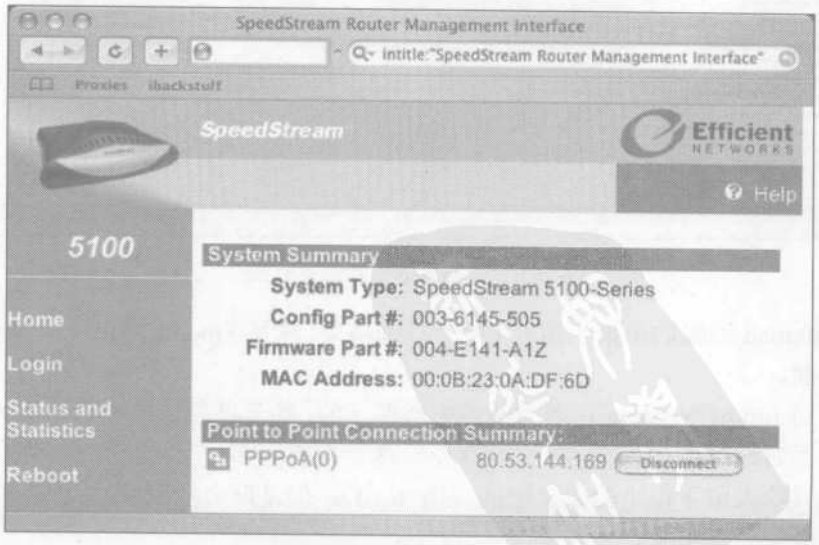


图 6.7　开放的快速路由器允许远程中断连接

当 m00d 提交查询的时候（图 6.7），说实话我没想到它能这么做。这个路由器绝对是由家庭用户安装的轻便设备，但我惊讶地发现它们在因特网上没有任何防护，大开方便之门。我个人很喜欢那个 Point to Point 列表内的按钮。今天想把谁的连接断开呢？

贝尔金（Belkin）是个家喻户晓的家庭用网络产品品牌。他们基于网页的管理界面很容易操作，这意味着如图 6.8 的网页会被 Google 所抓取。即使没有登录证明，这个网页还是暴露了很多让黑客感兴趣的信息。看到页面上的 Features 时，我笑了出来。防火墙开着，但无线网络正在打开且没有加密。作为一个有安全意识的黑客，我的第一本能就是将入口加密，尽力保护脆弱的家庭用户。

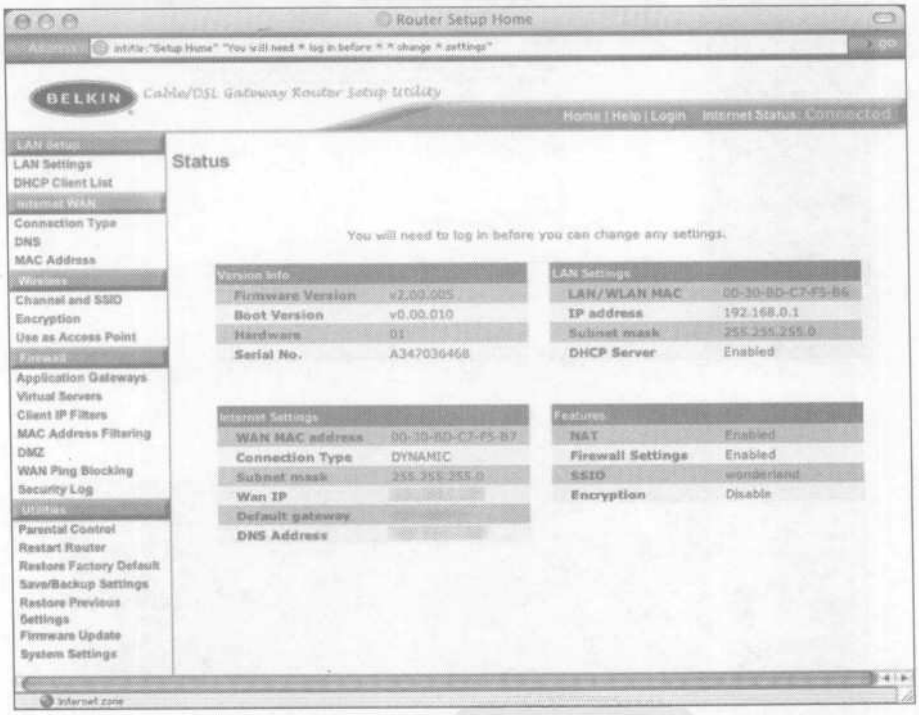


图 6.8 贝尔金路由器配置界面

Milkman 给我们带来了图 6.9 中的查询结果，这是 Smoothwall 个人防火墙的配置界面。

正如 Jimmy Neutron 在下面两图中所揭示的，甚至思科这样大名鼎鼎的设备，也会时不时地出现在 Google 的缓存中。尽管内容不多，交换机操作界面显示的信息也只给人留下很小的想象空间（图 6.10），但是所有的配置文件和诊断工具都在主页中列了出来。

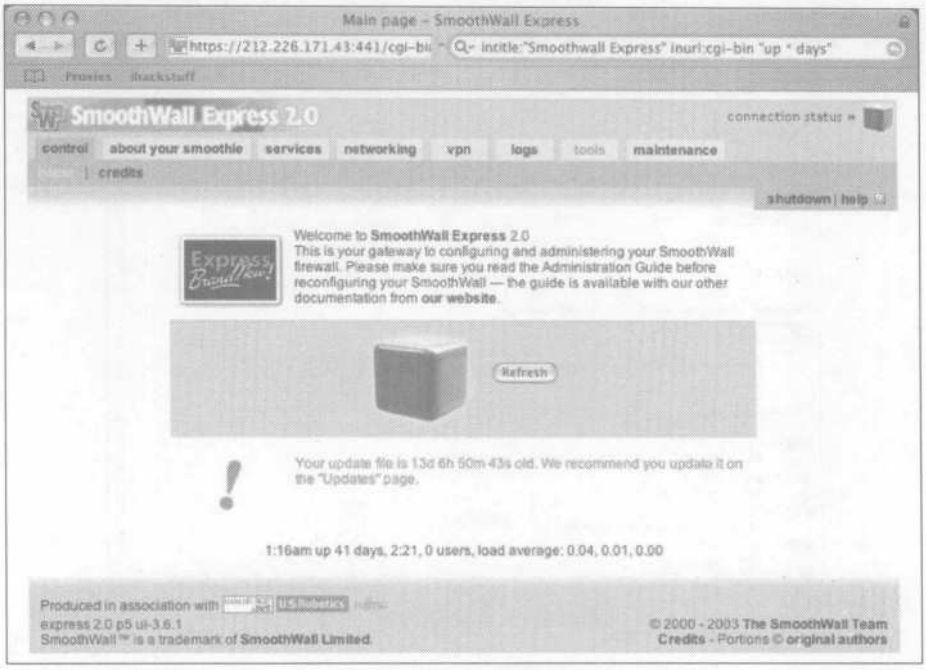


图 6.9　SmoothWall 防火墙需要升级

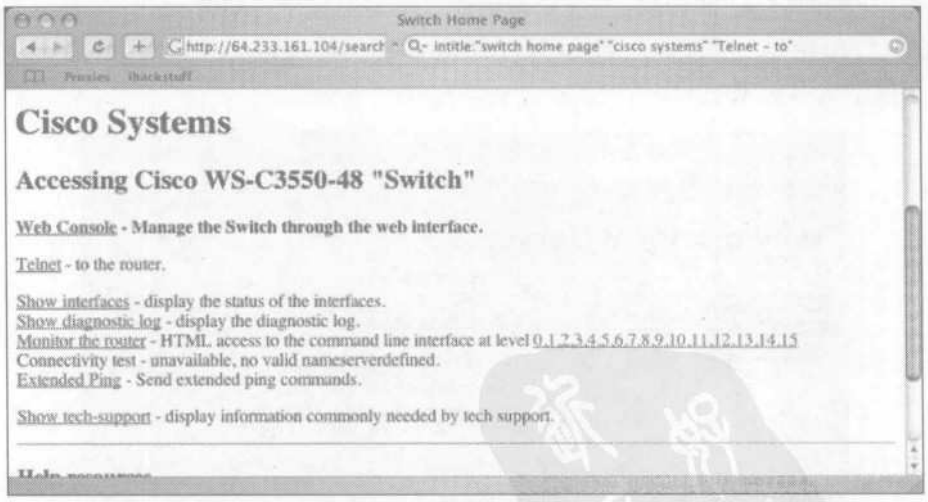


图 6.10　公开的思科交换机

第二张截屏应该是思科的设备。不知道为什么，思科对设备的命名让我想起一部好莱坞电影。我好像能听到影片中那种巨大的计算机合成的声音在召唤，“欢迎来到 15 级”（图 6.11）。

图 6.11 欢迎来到思科 15 级

图 6.12（Murfie 提供）显示的搜索结果找到了 Axis 网络打印机的操作界面。多数打印机设备的操作界面确实很无趣，但这个却引起我的兴趣。首先，这里有个名为“配置向导”的按钮，我确信单击它后可对设备进行配置。另外还有个 Print Jobs（打印任务）的链接，列出了打印任务。如果还没猜到，Google Hacking 有时不留下太多想象空间。

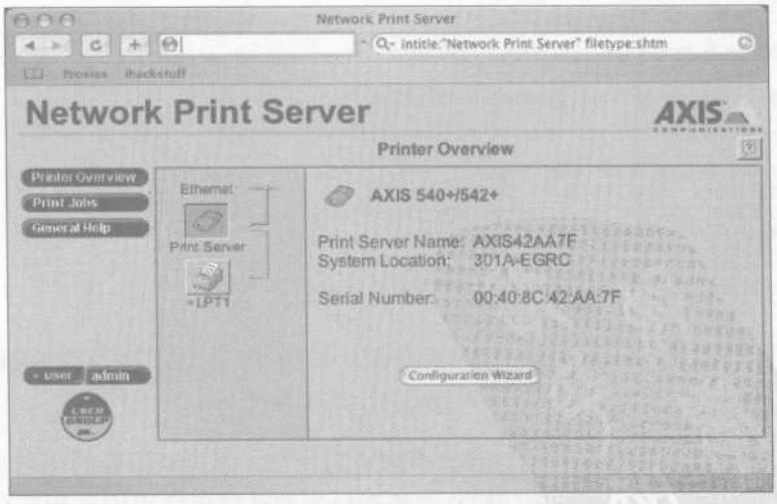


图 6.12 Axis 打印机服务器上的隐晦的按钮

打印机并不是完全索然无味。看看这个网页图片监视器（图 6.13），我尤其喜欢 Recent Religion Work 文档。除了将文件与兴奋剂联系在一起让人感觉不太好之外，那种追寻很有成就感。我发自内心地希望这两种事情之间没有联系。后来几天就没有什么让我惊奇的事情了。

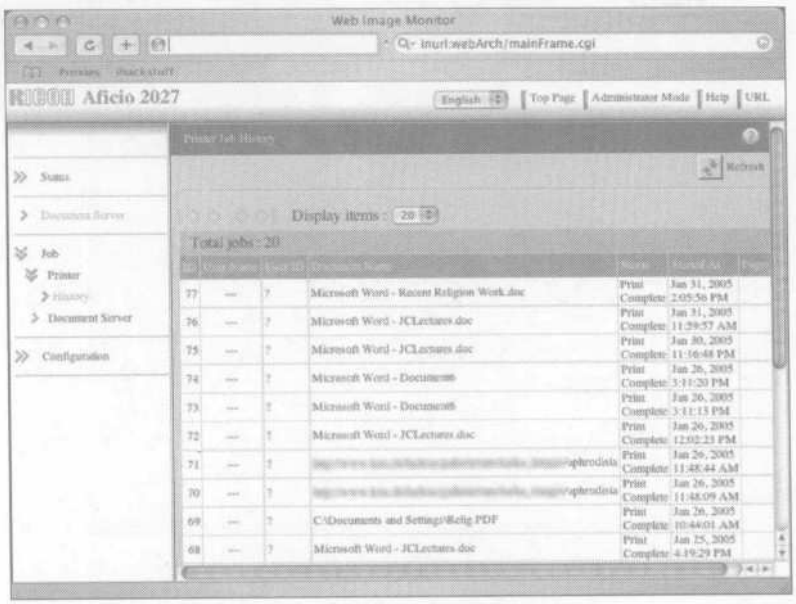


图 6.13 理光打印机服务界面

Cp 发现 Google 攻击的一个方法让我大笑（图 6.14）。这是一个喷泉的网页操作界面。

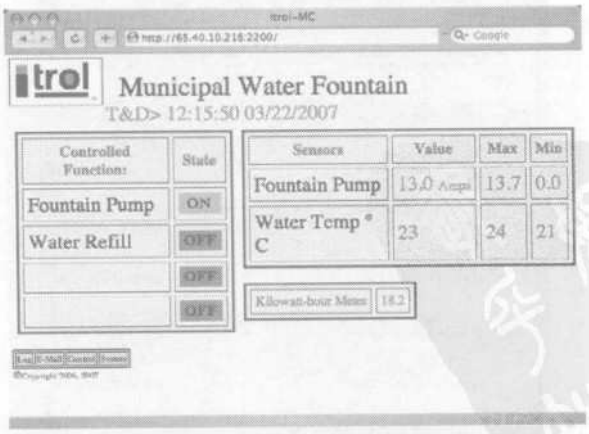


图 6.14 为了好玩和利益攻击喷泉

观察水温在一段密集时间内的浮动变化后，只需单击控制按钮，就能看能否真正操纵这个喷泉。正如图 6.15 揭示的，可以远程控制这个喷泉。

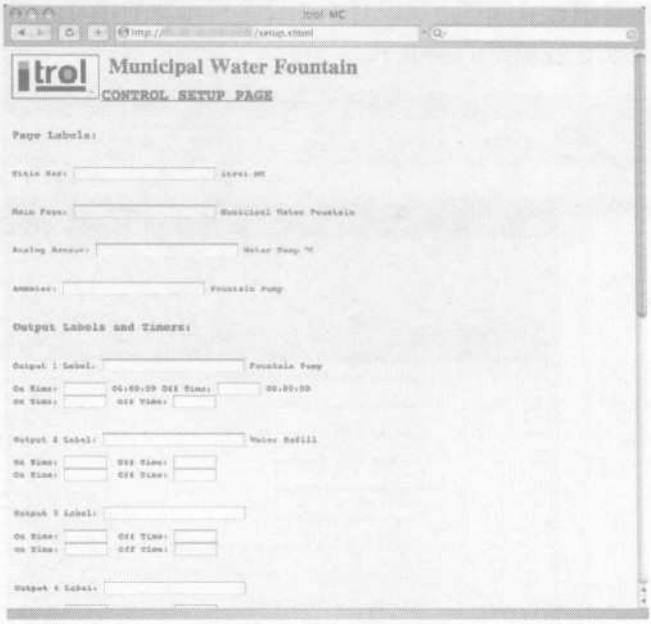


图 6.15 更多喷泉的趣事

我仍有个建议，如果碰巧进入了控制页面，要友好，不要变更储水系统的供电系统，那肯定会被认为是一次恐怖袭击。

看图 6.16，这个截屏上有比较多的控制设置。

图 6.16 Acid 上的 IDS 管理器

如今，我已经在安全行业里干了很多年，但并不是对此行业内任何一个领域了如指掌。有一件事可以很肯定，那就是安全产品是为了保护某物不受侵害而设计的。事情理应如此，但当看到一些如图 6.16 所示的日志这类东西时，完全迷惑了。要知道，这是一个入侵检测系统的网页操作界面。我最后又检查了一遍，数据应该保护完好，并不会被黑客发现，但还是觉得忽视了一封邮件或是其他什么东西。我以为这是符合系统操作逻辑的。如果入侵者看到自己把公共网页弄得乱七八糟，他会羞愧难当而不再入侵，会继续过自己平静的生活。如果是这样，可能他及其黑客朋友仅仅只是觉得运气好，这很难说。

开放的应用项目

许多主流的网络应用项目相对很容易被入侵，这是为了让对安全知之甚少的多数人操作更简单。即使这样，Google hacking 技术社区已经发现了很多网络应用程序是公开的，好像在等待着黑客来拥有它们一样。这部分的第一个例子是 Shadowsliv 提供的（图 6.17）。

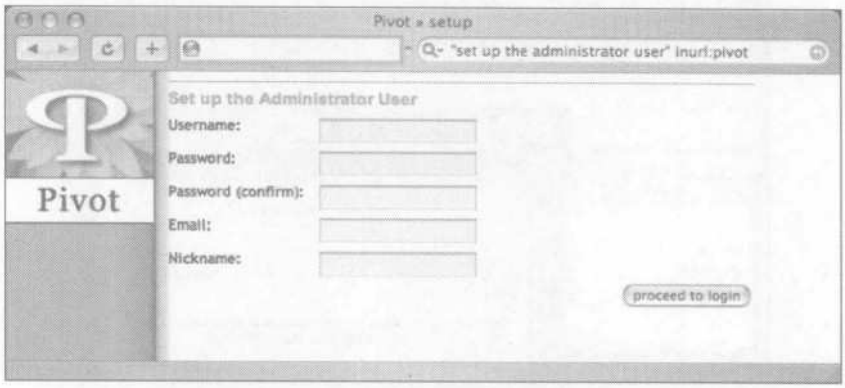


图 6.17　破解 Pivot 需要正确填写 5 个选项

坏消息是，如果黑客能够确定容易让人混淆的文本框里应该填什么内容，就会拥有自己的 Pivot 网页日志。好消息是许多技术不错的黑客不会入侵这个站点。黑客攻击可能就是简单地单击一下，这确实让人觉得难过，但是 Arrested 的研究表明要拥有整个网站其实是很容易的事，如图 6.18 所示。

比开放的 Pivot 安装少一个内容，这个配置页面将产生一个 PHP-Nuke 管理员账户，允许任何访问者上传内容就好像这是他们自己的网页一样。当然，访问者里会有不怀好意的人。实际上，他在创建一个管理员账户，可这个页面并非归他所有。可是，图 6.19 中网页上的文字就比较含糊了。

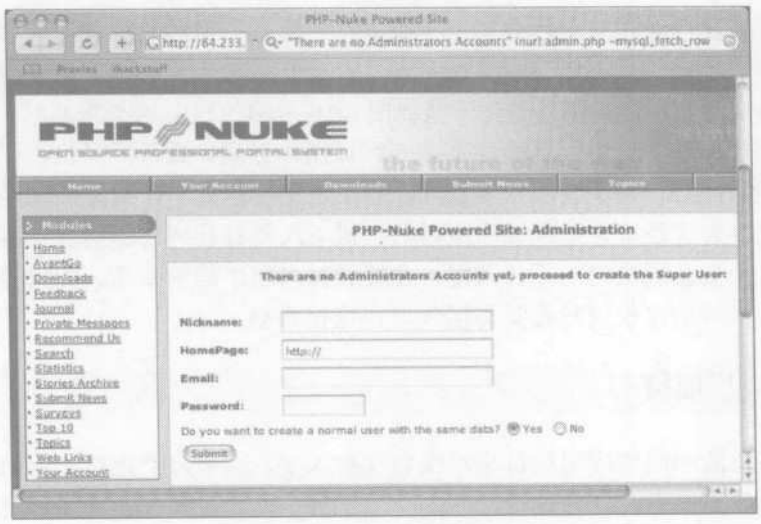


图 6.18 正确填写 4 个选项可获得 PHP-Nuke 所有权

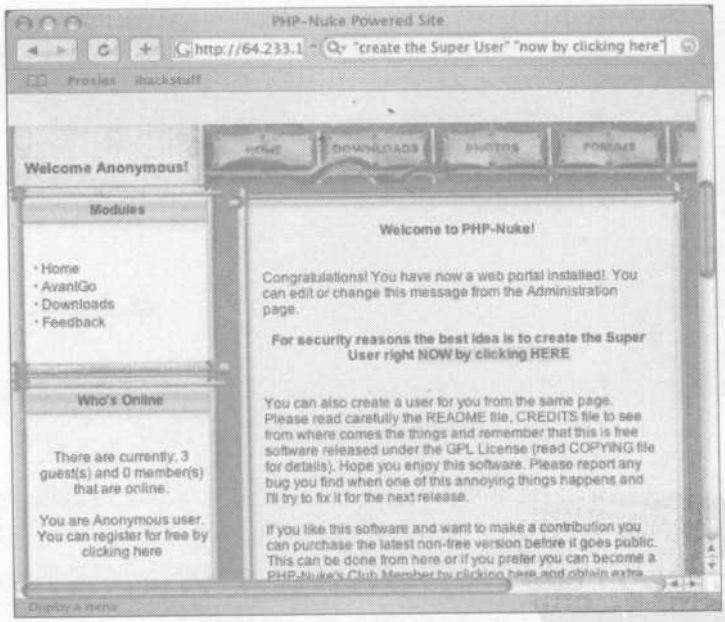


图 6.19 “出于安全原因”入侵 PHP-Nuke 安装

页面中间的粗体文字让我很气愤。我可以想象某人可怜的祖母看到网页上的文字也会大声读出来“为了您的安全，最好单击这里，马上创建超级用户”。我的意思是谁会出于安全的原因拒绝这样做呢？所有人都应该知道，他通过进入某些可怜虫的 PHP-Nuke 安装，或许能够将世界从黑客的攻击中拯救出来。

如果自己有个网站但不够酷，图 6.20 显示了一个 phpMyAdmin 安装程序，以根用户登录，提供 MySQL 数据库的无限制访问。

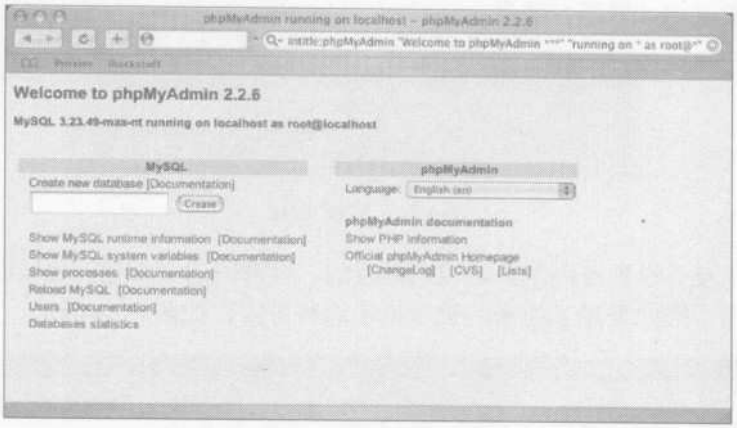


图 6.20　开放的 phpMyAdmin——蠢人的 MySQL 所有权

建立了网站，配置了 SQL 数据库之后，一个 Google Hacker 自然想最终控制整个系统。安装了 VNC，就可以远程控制一个系统的鼠标和键盘。如图 6.21（Lester 提供），这个搜索找到了 RealVNC 的客户端，它是基于 Java 的。

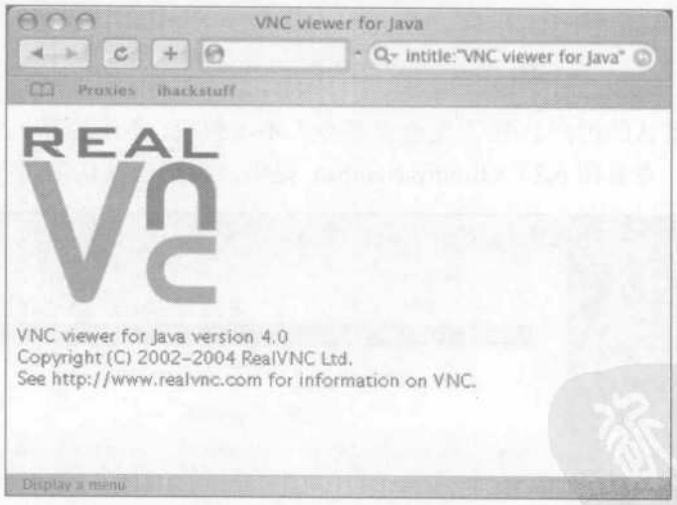


图 6.21　入侵一个 VNC，获取远程的键盘

但找到客户端只是一小步。黑客将仍然需要知道 VNC 服务器的 IP 地址、端口号、密码（不是必须的），如图 6.21 所示，弹出窗口中的 Java 客户端只提供三分之二的内容。

如果黑客确实走运，无意碰到一个服务器没有密码保护，会面对图 6.22 中连接窗口这样让人畏惧的任务，4 个按钮中应该单击哪个呢？这里是新手的小提示：不要选择 Cancel（取消）就行。

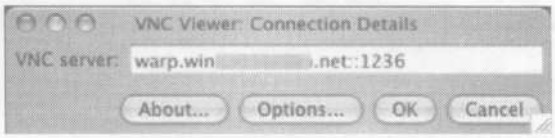


图 6.22 VNC 选项

当然，没有设置密码保护是相当愚蠢的。但密码这么难记，卖软件的显然知道这个问题，因此采用了为密码设置提示这种方式，如图 6.23 所示。

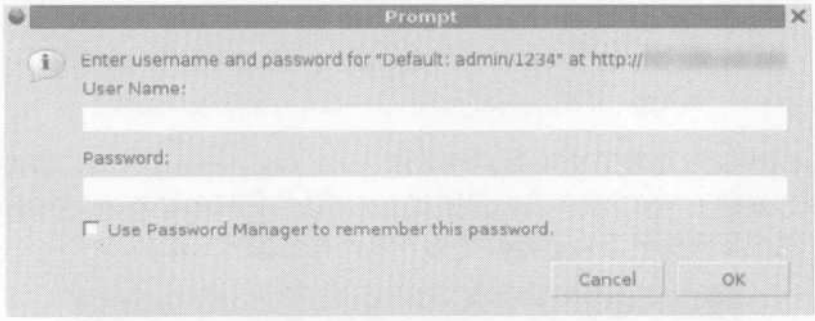


图 6.23 容易取得的密码提示，以防黑客们忘记

显示出默认的用户名/密码组合真是令人不可想象。不幸的是，这个过程不是单独的事件。查看图 6.24（Jimmy Neutron 提供，能猜出默认密码吗？

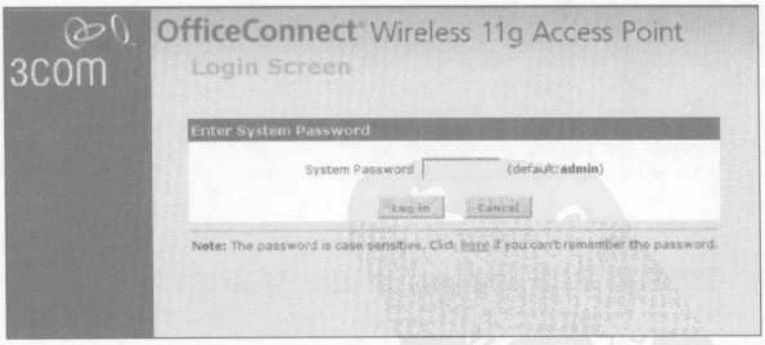


图 6.24 如果猜不出默认密码就蠢死了

想要进一步提高的黑客的接下来就需要努力了。仔细看图 6.25 所示的用户屏幕截图（Dan Kaminsky 提供）。

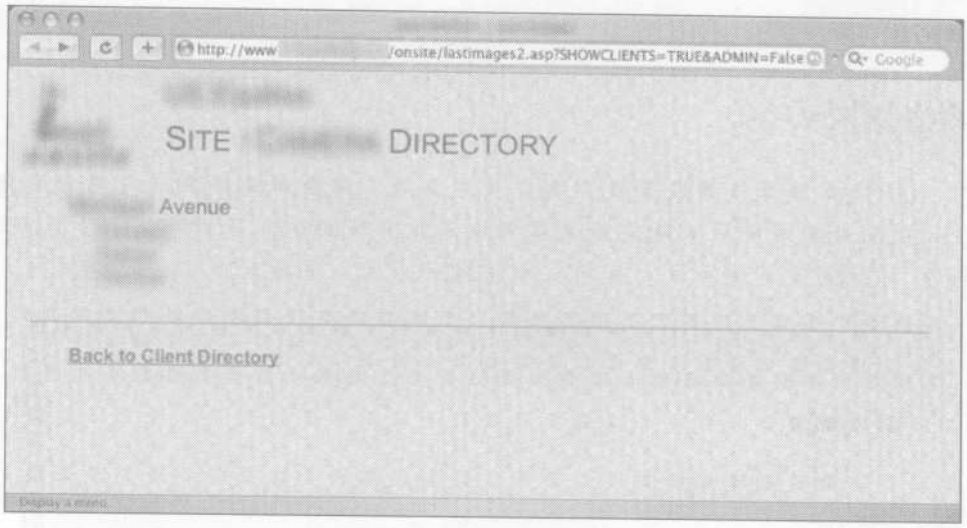


图 6.25　欢迎来到 Guest Access

如果看得比较仔细，会注意到 URL 中包含一个特殊的字段（ADMIN）被设置为 False。像黑客一样思考，怎样能获得管理权限以进入这个网页？见图 6.26。

图 6.26　通过改变 URL 获得 Admin 登录权限

仔细看图中新出现的 Exit Administrative Access 按钮。通过改变 ADMIN 字段，使它为 True，应用程序就将我们带进了管理权限的模式。黑客入侵真的很难，我发誓。

网络摄像头

说实话，我承认就像搜索打印机一样，不喜欢搜索网络摄像头。这里添加进GoogleHacking 数据库(GHDB)的都是网络摄像的查询结果。有些网络摄像头相当有趣，值得在这里提一下。我先从手机摄像头讲起，如图 6.27（Vipsta 提供）。

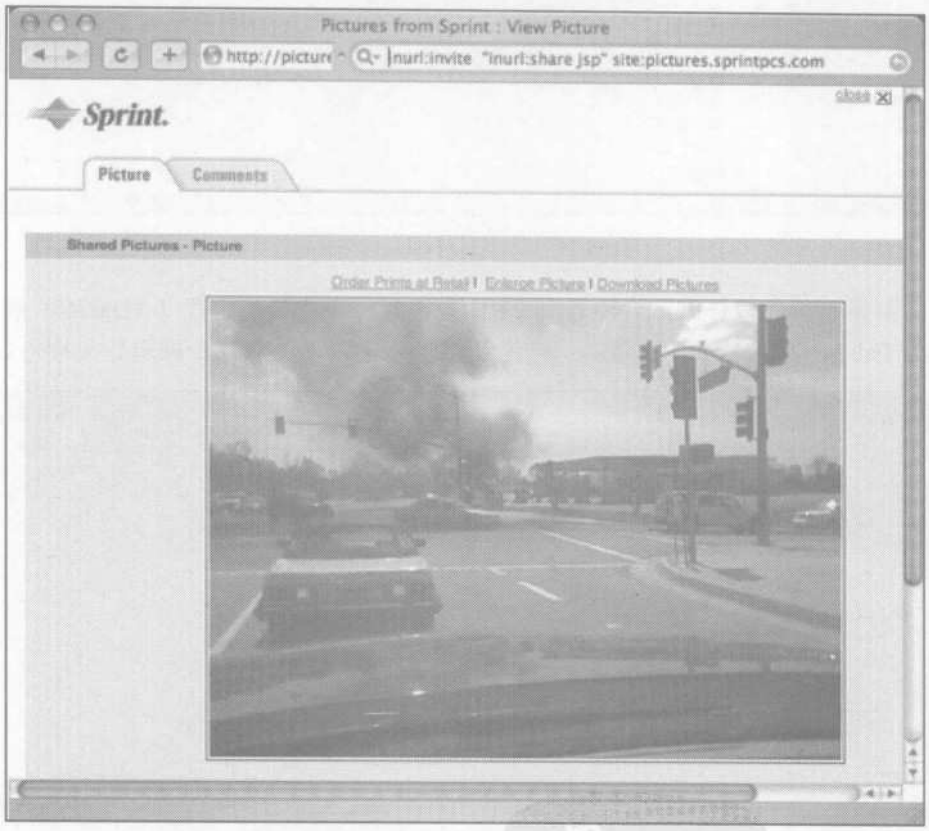


图 6.27 Google 收录的交通事故

这不仅是张严重的汽车交通事故的照片，而且 Google 收集图片的网站的构思很有趣。谁知道会有什么样的照片可以作为勒索的素材呢。并不是任何人都会为了经济或感官上的目的使用那种类型的信息。

继续，仔细看下面这个安放在办公室里的网络摄像头，如图 6.28（Klouw 提供）。

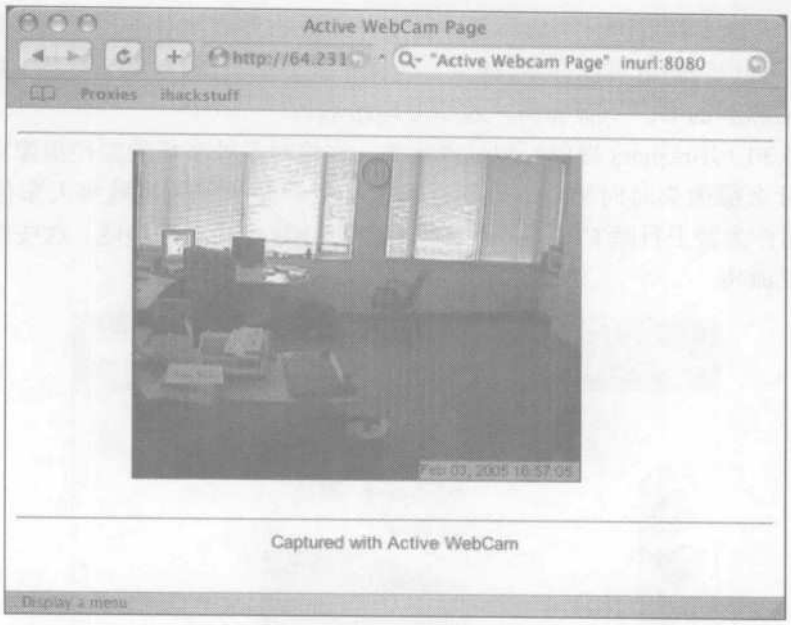


图 6.28　远程背后偷窥

这确实是一个有趣的网络摄像头。不仅可以看到办公室里所有的活动，而且看似专门为远程背后偷窥的进行而设计的。以前，黑客们不得不在走出房间才能这样做，而现在，只需用 Google 找到他们需要的摄像头就行了。

图 6.29（Jimmy Neutron 提供）显示了美国战略核潜艇的设计构造。

图 6.29　不是真正的美国战略核潜艇

是的，这不是真的。大概只是个核反应堆或动力控制中心，或者一个位于哥伦比亚（马里兰）的毒枭的仓库。或许是我读了太多的类似《从网上盗窃》（*Stealing The Network*）的书。不管如何，这个发现很酷。

图 6.30（JBrashars 提供）却是真实的，这绝对是停车场的监控摄像头。我不确定为什么摄像头对向了一个残疾人车位，大概是为了监视残疾人车位被占用吧。设想作为警卫目睹 CIO 停车、跳出轿车并跑进大楼的乐趣吧。这些在安全警卫中广泛流传。

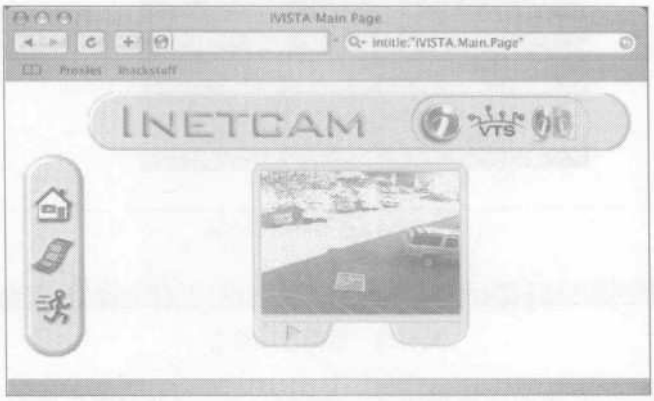


图 6.30　停车场的残疾人车位监视器

图 6.31（WarriorClown 提供）显示的是一个装运码头，地上摆满了白色的易爆的容器。

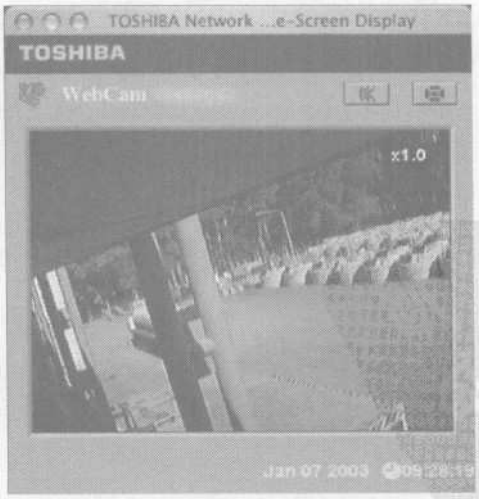


图 6.31　远程引爆容器很有趣

虽然开始看起来没什么意思，但网络摄像头确实很有趣。我敢肯定单击右上方那个按钮会向那些白色容器发射出激光束，足以制造事故，但只能做一次——除非将它们设置成重复的，可以让它们自动恢复，当然，这只能在 Halo 3 这个游戏里有效。所有的网络摄像头让我有些搞不懂了。为检验我的设想正确与否，提供一些涉及安全摄像头的照片（图 6.32）。

图 6.32　公开的网络安全摄像头

将公开的摄像头放到网上是愚蠢的，不只有我这样想。当然，好莱坞电影里经常上演这样的镜头，好像雇来黑客就是为了接入视频监视录像。但电影里将这些过程制作得很复杂，好像对技术要求很高。我从未看过一个好莱坞电影里的黑客利用 Google 入侵一个安全系统。如果那样，就不会像纤维光学摄像头、剪钳、弹簧夹那么酷了。

继续，如图 6.33 所示（JBrashars 提供）的搜索显示了一些公开的 EDSR 应用程序。

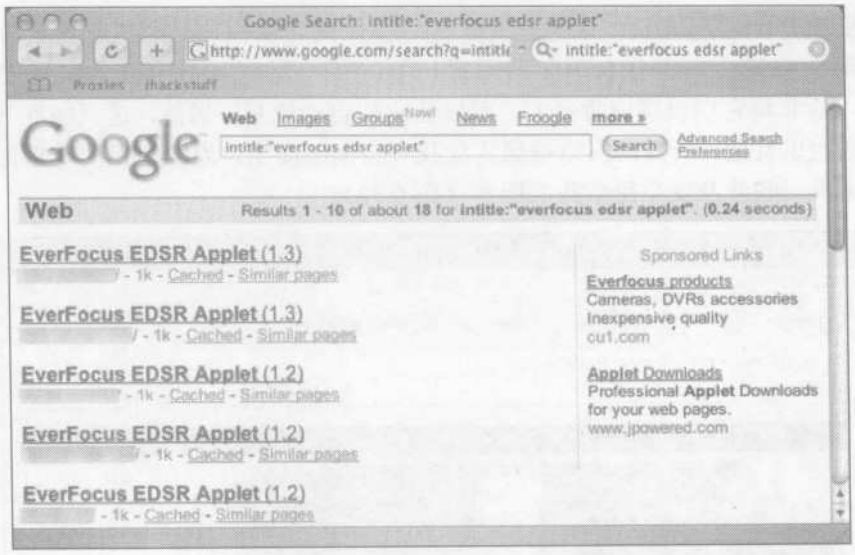


图 6.33 EDSR 听起来很一般

Everfocus EDSR 是一种多通道的数字视频录制系统，有一个基于网页的操作界面。这是个正宗的监控产品，因此有默认的密码保护，如图 6.34 所示。

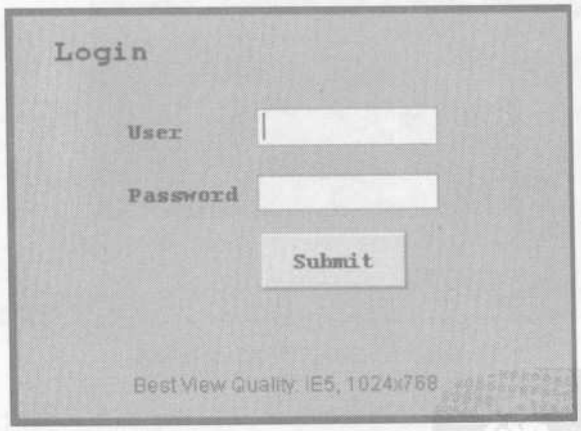


图 6.34 密码保护：安全黄金法则

不幸的是，因为是匿名人士提供的，通过出厂时默认的管理员用户名和密码就可以进入许多这样的系统，如图 6.35 所示。

一旦进入系统，EDSR 应用程序可以接入多个现场监视画面，以及之前的历史记录。就像好莱坞电影中的神奇场景一样，不过略去了所有黑客的入侵过程。

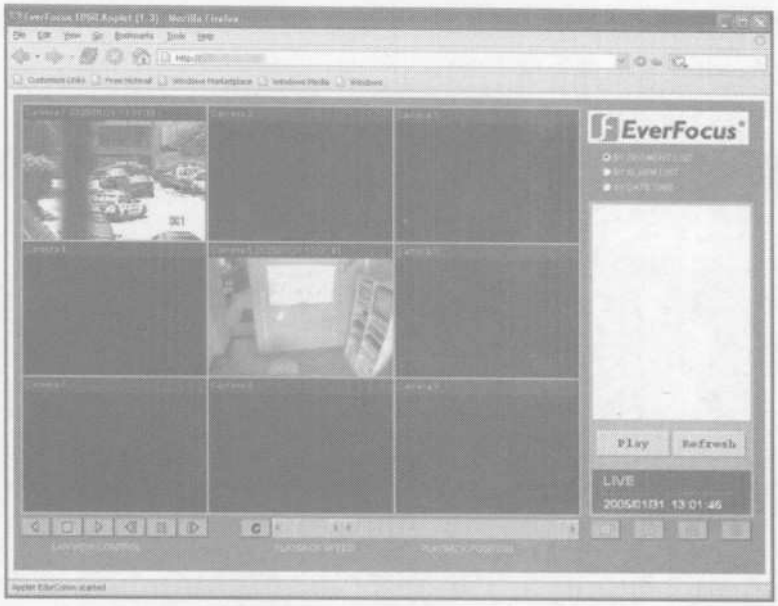


图 6.35　欢迎来到监控中心

EDSR 不是 Google 攻击的唯一的多通道视频系统。Murfie 透露说，搜索 I-catcher CCTV，得到许多如图 6.36 所示的系统。

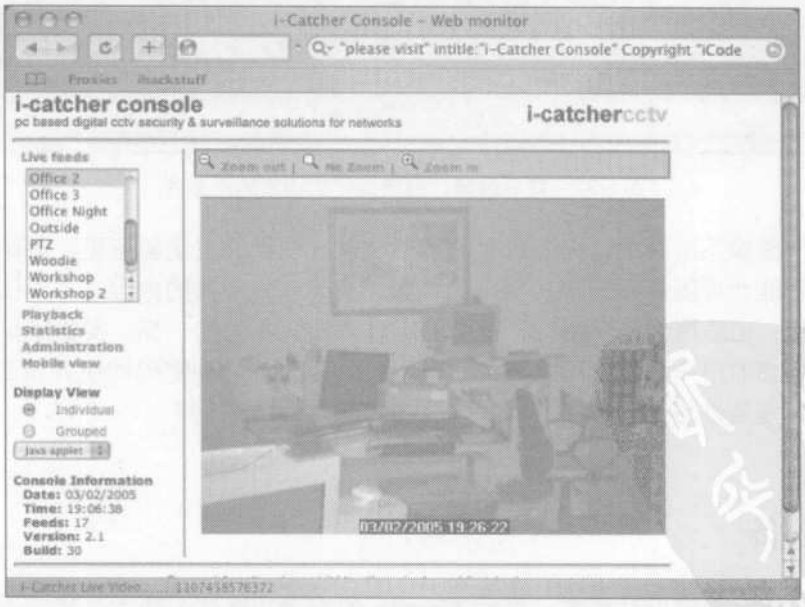


图 6.36　网络监视画面

尽管界面可能有点简单，但提供许多摄像头的现场监视的访问链接，包括一个叫作“Woodie”的，我不敢单击它。

这些摄像头都很有趣，但是我把最喜欢的留在最后。如图 6.37。

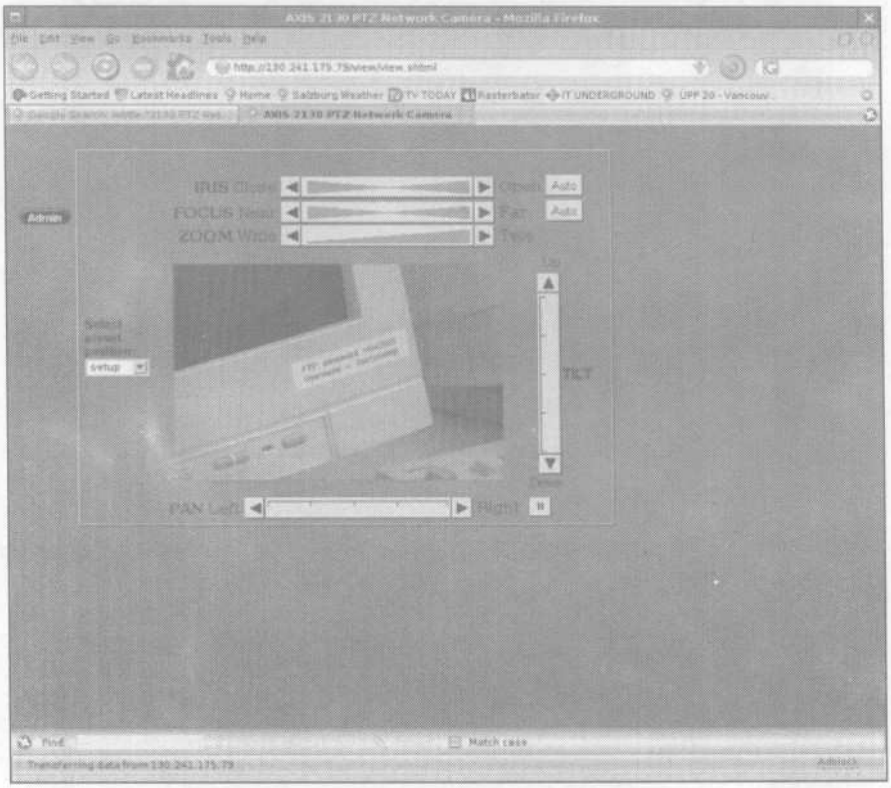


图 6.37 背后偷窥、网络摄像头和密码跟踪者

这个摄像头给网络访问者提供开放的链接。在计算机实验室里，摄像机的远程控制功能允许匿名用户观察周围的场景，搜寻放大想找的内容。它不仅适用于背后偷窥，也适用于密码跟踪，上面的屏幕截图让我大吃一惊。实验室里在线的 FTP 服务器的用户名和密码都被列出来了。列出用户名和密码的便签相当糟糕，但我想知道是谁想到这样好的点子，将摄像头对准了它们？

电信设备

我从来没做过电话黑客，多亏 Google 的搜索功能这么强大，我才不用干那种工作。从 JBrashar 提供的搜索结果（图 6.38）可以看出，建立在 IP 服务之上

的语音通话技术（Voice over IP, VoIP）已经很受欢迎，这也带来了很多基于网页的电话操作界面。

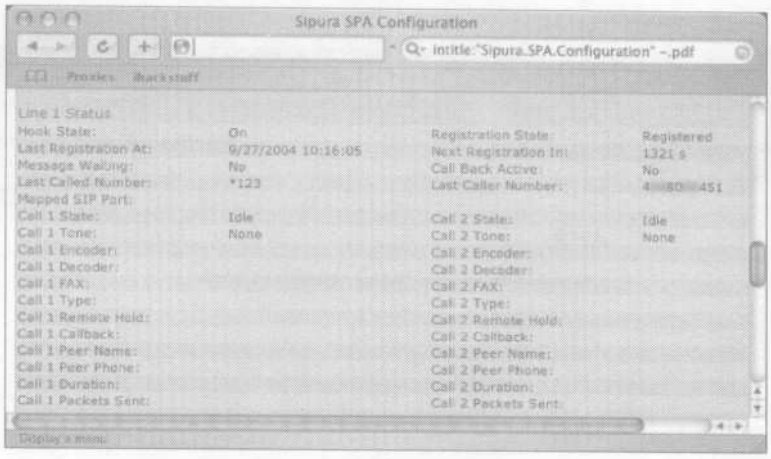


图 6.38 Google Hacking 居民电话系统

对我来说这很有趣，一个黑客只需借助 Google 就能得到某个电话的通话记录，如最后一个呼叫的号码和最后一个来电号码。通常，Sipura SPA 软件可以很好地保护这些通话信息，但这个特殊的安装程序没有正确配置。另外，更多的技术信息也可以通过单击网页操作界面上的链接来得到，如图 6.39 所示。

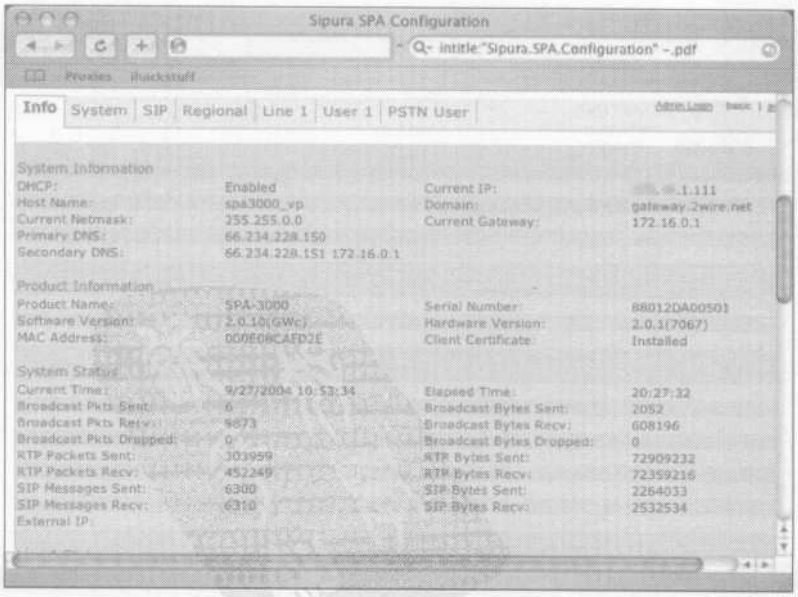


图 6.39 Redux

VoIP 设备太多了，本书不可能涵盖全部，但针对 VoIP 服务器组只有 Asterisk。查看了 Asterisk 的管理入口文件之后，Jimmy Neutron 提供了图 6.40 显示的有趣的搜索。

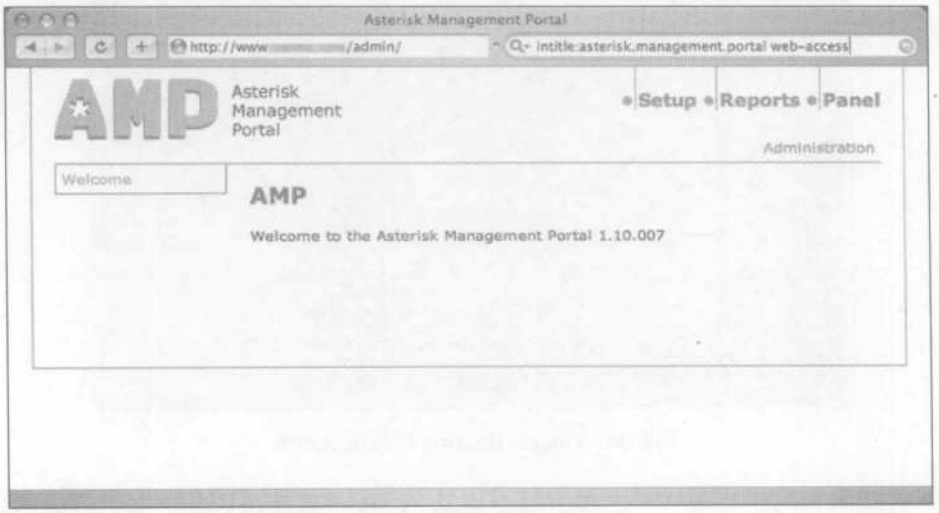


图 6.40 Asterisk，VoIP 之王

通过这种开放的方式，黑客可以对 Asterisk 的服务器进行修改，包括预设来电，如图 6.41。

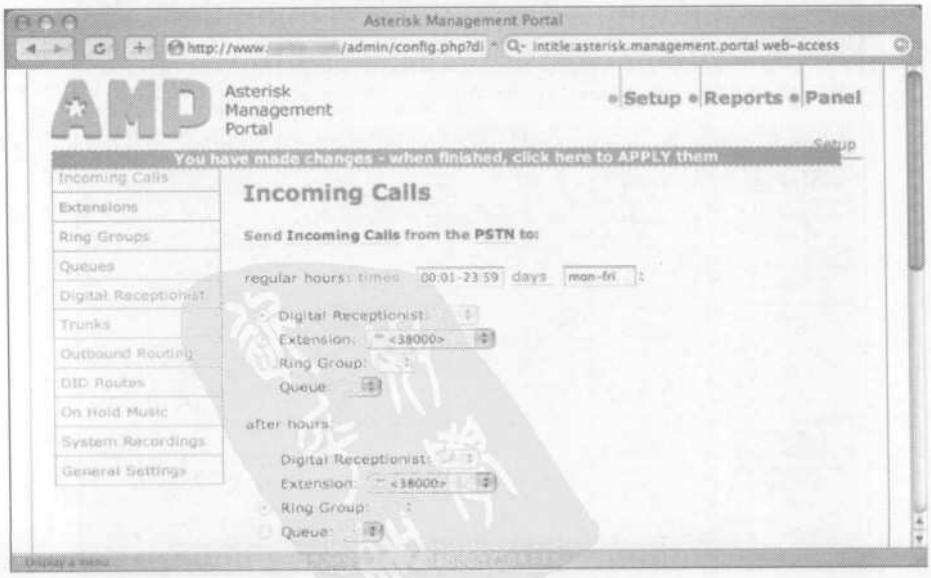


图 6.41 Google Hacking Asterisk 管理入口

不幸的是，黑客兴趣并未就此止步，他可以重新配置扩展组件、监视器设置、换道发送语音邮件、打开或禁用信号接收器，甚至上传扰人的音乐。但是Jimmy对Asterisk VoIP功能的挖掘还在深入；后来又提供了下面的搜索结果，如图6.42。

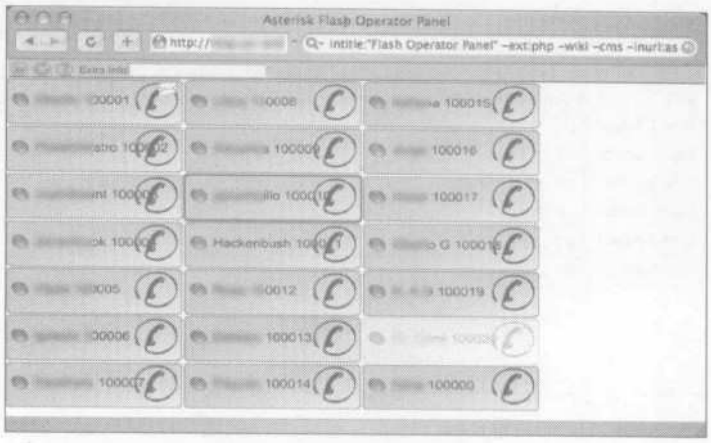


图6.42 Redux. HackenBush. Heh

基于Flash的操作面板提供了类似的功能，同样对所有的网络用户是开放的。

还有，Yeseins提供了一个有趣搜索（图6.43），找到了一些视频会议管理系统。

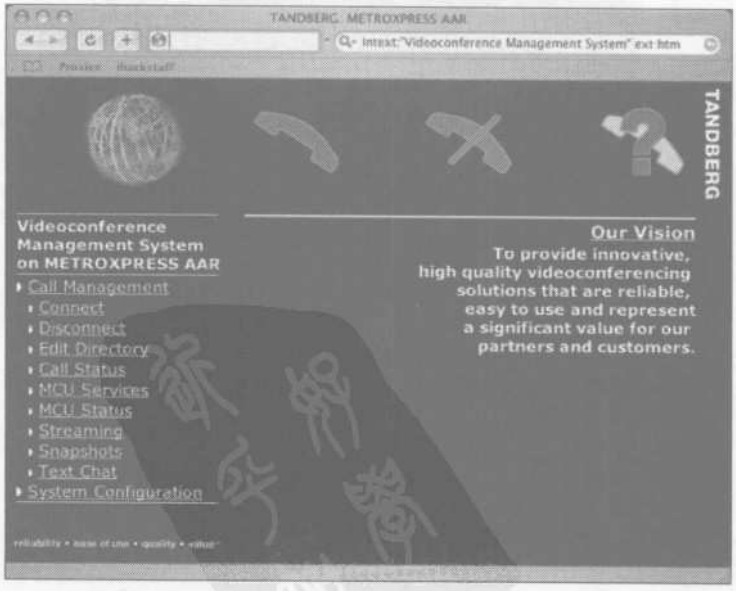


图6.43 是否是黑掉视频会议系统

这个管理系统允许网络用户建立会议连接、撤销会议，以及监视会议电话、拍摄会议参与者，甚至变更线路设置，如图 6.44 所示。

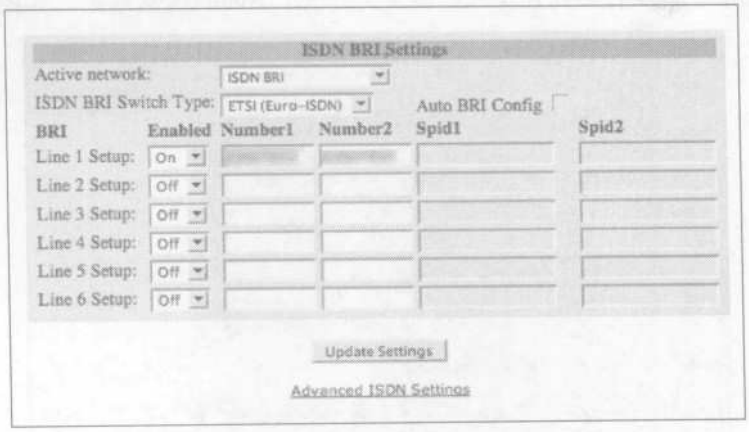


图 6.44 重设定视频会议线路

有恶意的黑客甚至能改变系统名和密码，锁定系统合法的管理员，如图 6.45 所示。

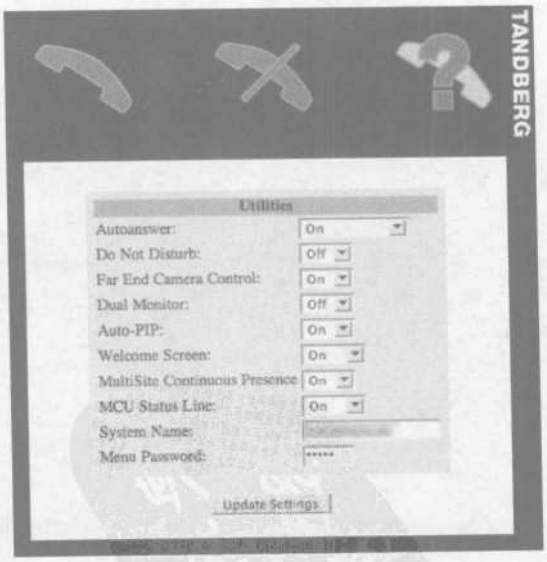


图 6.45 视频会议系统所有权

尽管看了这么多新型的网页操作界面，Google hacking 技术也能用于以前的系统。如图 6.46 所示。

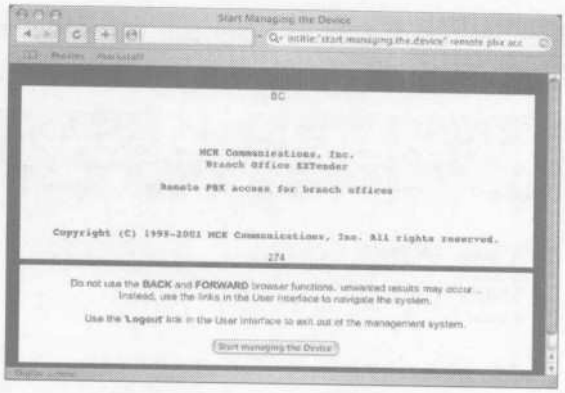


图 6.46 基于 Google 的电话线盗用

这种前端界面设计是为老式的 PBX（数字程控交换机）产品包装外表，但客户的安全似乎摆在了次要的位置。注意到这个界面要求使用者“退出登录”，暗示着用户已经登录。另外，注意那个含义模糊的按钮，“Start Managing the Device”（开始管理设备）。一个有恶意的黑客，在使用 Google 搜索到相关信息后，要做的就是确定单击哪个按钮。多么让人难以置信啊。

电源系统

在谈到用 Google 入侵电源系统时，许多人皱起了眉头。大多数人认为我说的是不间断电源系统（uninterruptible power system, UPS），如 Yeseins 提供的图 6.47。

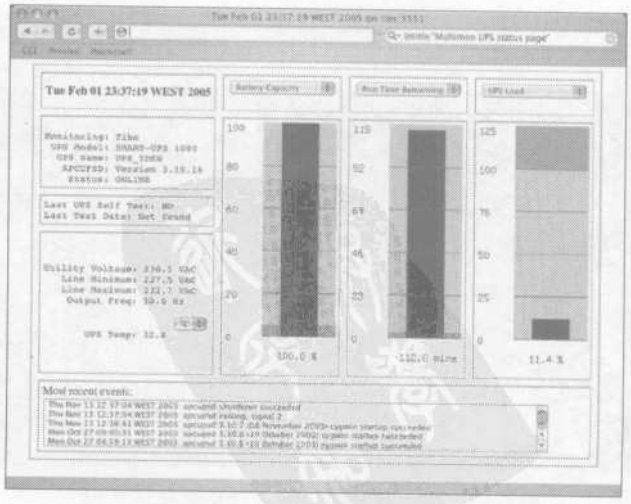


图 6.47 是否是 Whazzups

这个查询很聪明，但只是个 UPS 的监视页面。但是如 Jimmy Neutron 提供的图 6.48，有更多有趣的入侵电源系统机会。

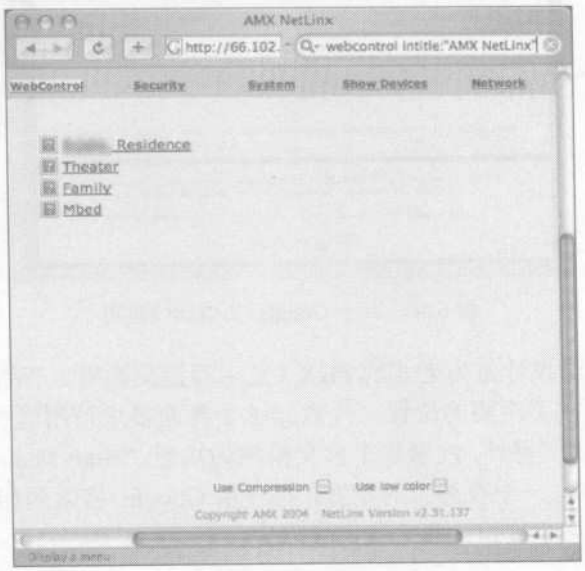


图 6.48 卧室里的入侵行为

AMX NetLinx 系统的设计目的是管理控制电源系统。上图中似乎是建议访问者在剧院、家中、主卧室里控制电源系统。问题在于，利用 Google 搜索到的结果很少，而且大多数是密码保护的。Jimmy 提供了如图 6.49 所示的搜索结果，可以作为一个备选方案。

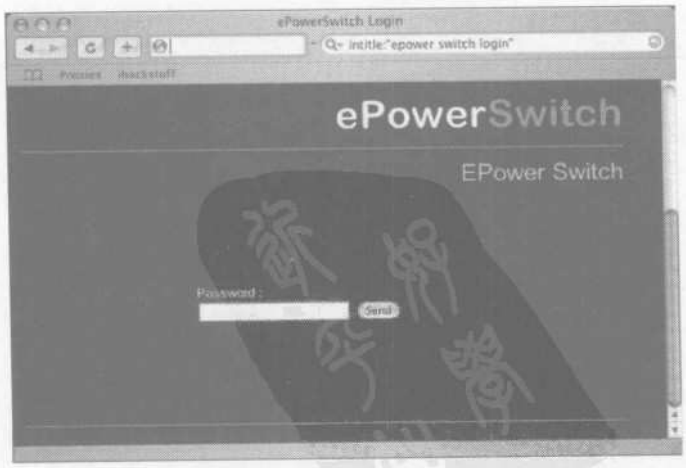


图 6.49 密码设置的记号，特别是默认密码

这个搜索结果找到一大串密码保护的网站，而且许多站点仍然使用默认密码进入控制面板，如图 6.50 所示。

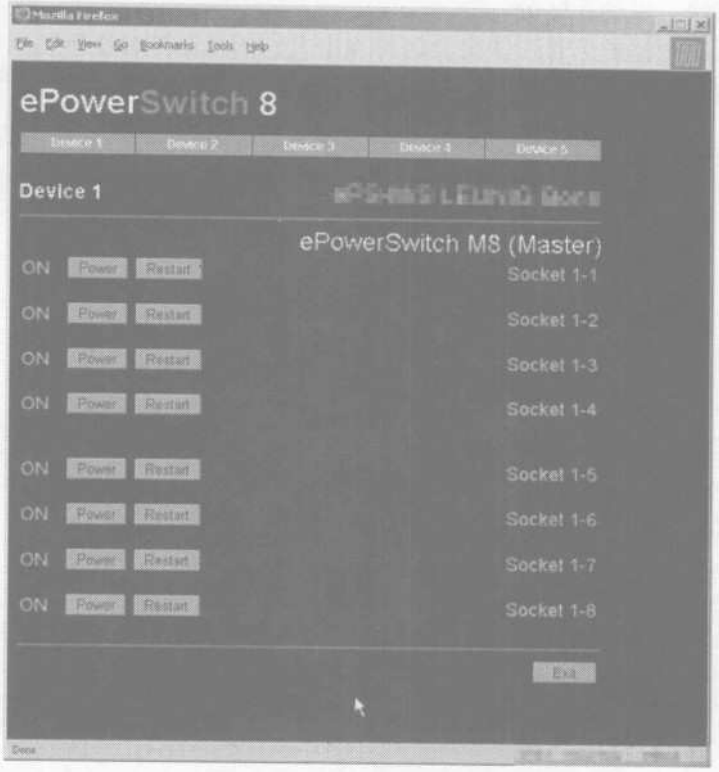


图 6.50 是否是 Google Hacking 电灯插座

这个控制面板上列出很多电源插座，旁边是些有趣的按钮，称为电源（power）和重启（restart），技术再差的黑客也明白是什么意思。这种操作界面的问题是单

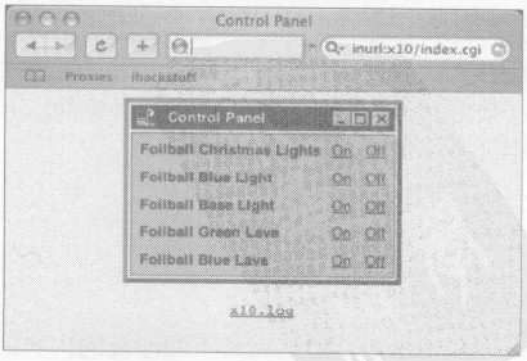


图 6.51 远离圣诞灯饰

调无趣。黑客肯定对开关电源按钮感到厌烦，除非找到了一个网络摄像头可以看到一些有趣的事情。如图 6.51 所示的搜索看起来是说明这个问题的，每个灯具都有自己的名字，以便于区分。

即使最不道德的黑客可能也会认为攻击人们的圣诞灯饰是粗鲁无礼的，但任何头脑清楚的黑客都不会拒绝如图 6.52 所示的公开的 HomeSeer 控制面板。

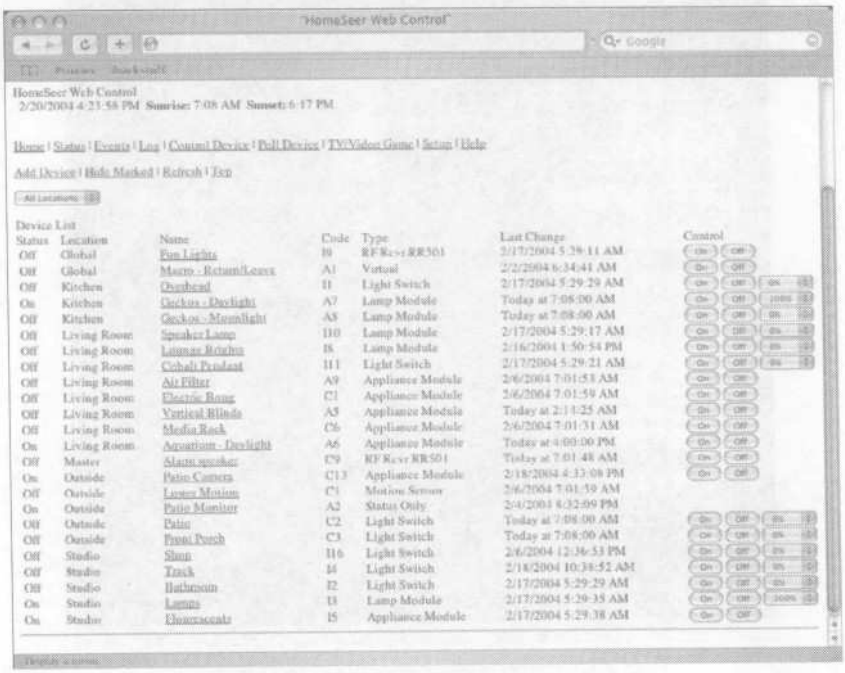


图 6.52 家用电子产品入侵

HomeSeer 控制面板使攻击电源又变得有趣了，每个控制开关都有相关的描述信息，开（on）、关（off）以及应用部件上的滑动开关。有些部件很有趣，可以控制光强和盥洗室的照明。最有趣的当然是家用电子产品。如果为情报机关工作，想要抓捕系统所有人，我建议先用 Google 攻击，再进入他家。首先将灯光调得比较昏暗，接着锁定动作传感器。最后但不是必须的，万一其他攻击没有效果，可以入侵他家中的电子产品。

敏感信息

敏感信息只是个一般性术语，但这就是下面涉及的内容：使用 Google 搜索，会得到大量的敏感信息。首先看 Jorokin 提供的 VCalendar 搜索得到的结果，如

图 6.53 所示。

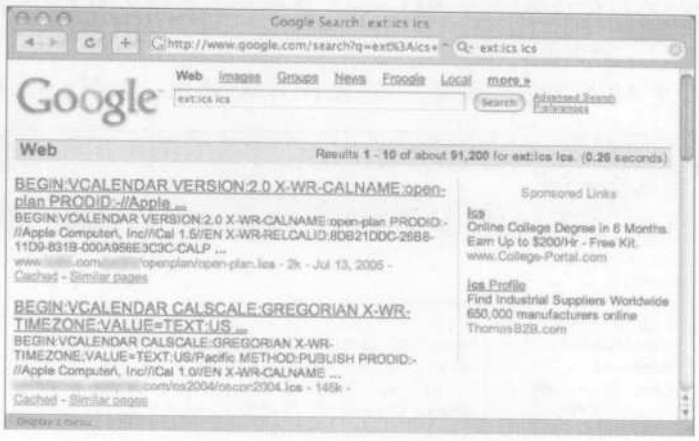


图 6.53　让我来检查他们的日程表

至少有这种可能，这些日程文件被专门做成公开的，但是 Netscape 的历史文件不应该是公开的。如 Digital_Revolution 提供的如图 6.54 所示。

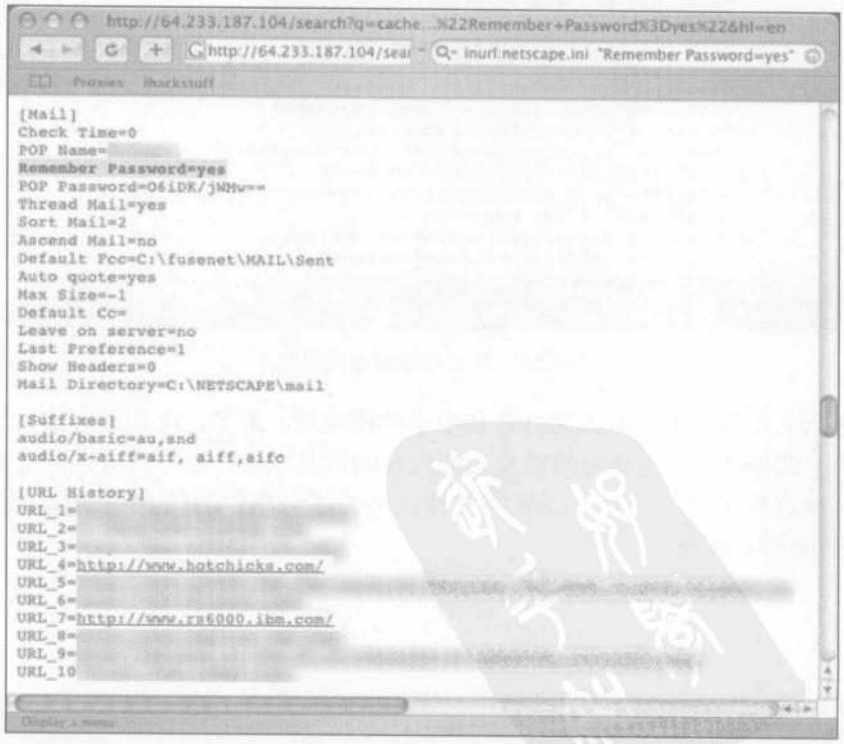


图 6.54　IBM 的美女？并非如此

对新手而言，文件包含使用者的 POP 电子邮件的用户名和密码。还有，他的 URL 历史记录不仅包含著名的 IBM.com，还包括不太知名的 hotchicks.com，我肯定这是不适合上班时间浏览的。

下面是一个 MSN 联系人列表，由 Harry-AAC 提供，如图 6.55 所示。

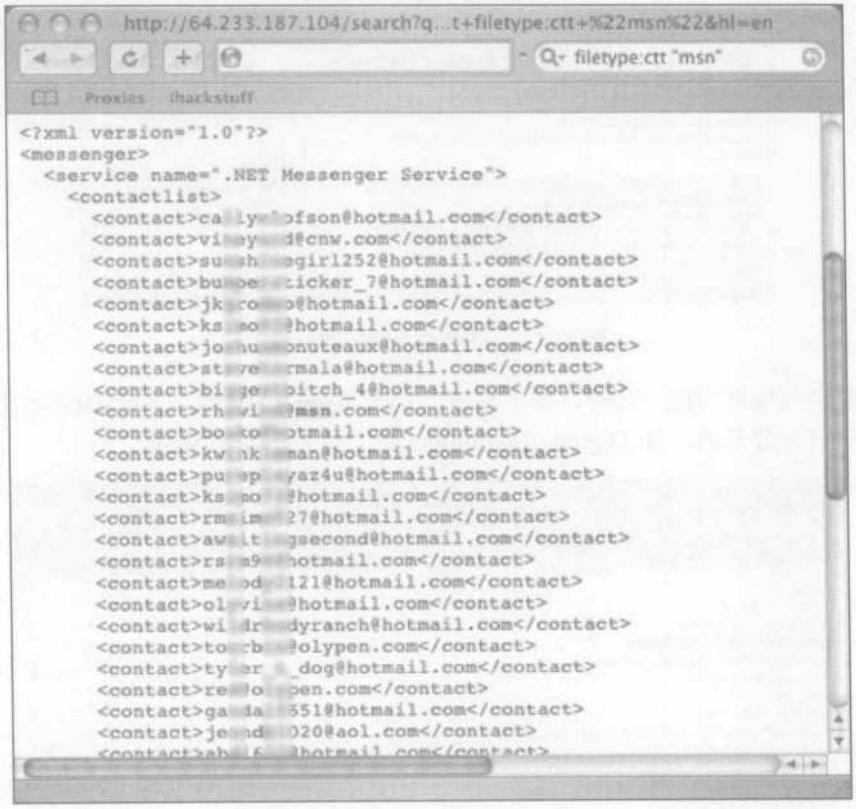


图 6.55 是不是想偷走我的朋友

这个文件列出了联系人的姓名和电子邮箱地址。最多，这是垃圾信息。网上包含电子邮箱地址、电话号码以及其他内容的信息很多，但令人惊讶的是有多少文件包括这种类型的信息，而这些文件又是为了分享这种信息而新建。看看由 CP 提供的图 6.56 吧。

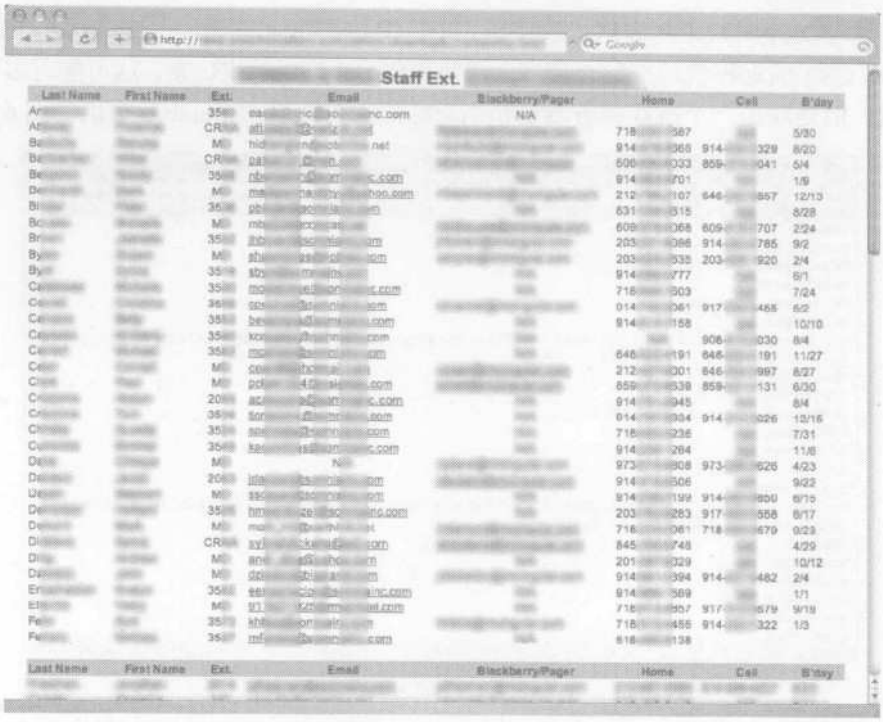


图 6.56　打电话或发邮件给所有员工，祝他们生日快乐

这个文件是一个员工名录，只是为了内部使用而创建的。唯一的问题是可以在公开的网站上能找到它。这个看起来并未涉及太多的私人信息，但如图 6.57 所示的搜索结果就透露了相当多的敏感信息：密码。

图 6.57　RCON 密码

这个文件罗列了文本格式的密码，属于 Ghost Squad 的私人反恐精英（Counter Strike, CS）的远程管理控制台程序。问问任何一个 GS 游戏玩家，这可能有多么的麻烦。但是攻击一个游戏服务器是相当乏味的。下面看由 Barabas 提供的图 6.58。

图 6.58 加密的 VPN 密码

这个文件列出了一个思科的虚拟局域网（VLAN）的信息和加密的口令。比暴露 VLAN 的加密的口令更严重的是暴露 VLAN 的文本格式的口令密码。尽量用 Google 搜寻，会有收获的。查看同样由 Barabas 提供的图 6.59。

图 6.59 普通文本格式的 VPN 密码

是的，那是安置在一个大学的配置文件中的文本格式的密码。但是，有趣的密码可能在很多地方找到，如在 Windows 的自动安装文件中，如 MBaldwin 提供的图 6.60。

图 6.60 在安装前确保系统是 Windows 系统

这个文件里还有安装软件的产品验证码，可用来合法地重新安装软件。最后，但并非最不重要的，看由 CP 提供的图 6.61。

文件罗列了很多网站的用户名和密码。它被储存在一个网站上，大概允许所有者可以方便地远程获得。然而，文件位置是公开的，Google 能搜索到它。记住，公开的网站一般是这样——公共的。不要不经过深思熟虑就将公开的数据和私有的数据混合在一起。

警方报告

据我所知，大部分警方记录是公开的。所以看到如图 6.62 所示的警方报告时，我并不惊讶。

然而，看到下面这个警方报告（图 6.63），我开始质疑公开记录的合理性。

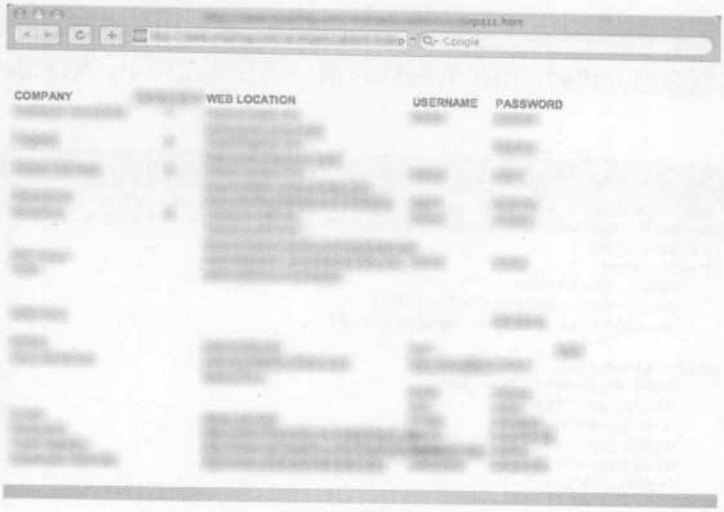


图 6.61 嗨，我能得到你所有的网页密码吗？

图 6.62 警方报告是公开记录

图 6.63　这也意味着银行秘密账户信息

这个警察报告记录了一个小偷偷窃一个妇女的钱包的细节。问题是，妇女钱包里的东西被详细地列了出来，包括她的银行信用卡的账号！这种过分详细的警察报告情况在网上并不少见。图 6.64 所示是另一个例子，暴露了更多信息。

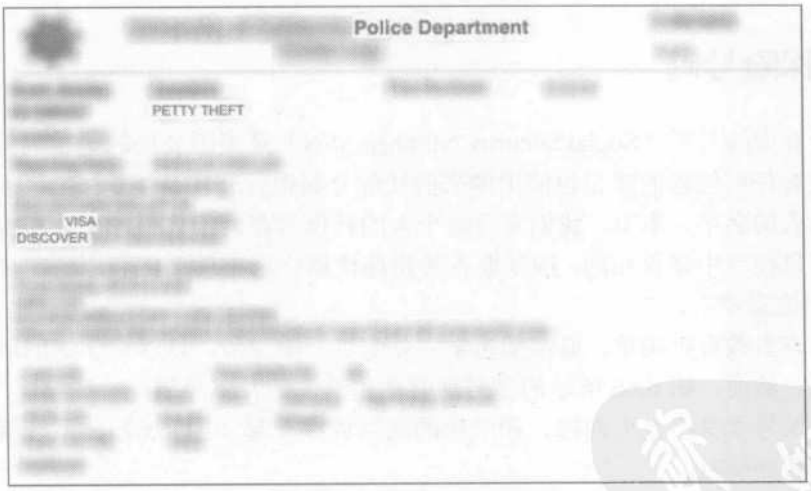


图 6.64　抢劫两次，多亏公开的警察记录

这个报道详细记录了另一个偷窃案例，这次将被盗的 Visa 信用卡号和 MasterCard 信用卡号都公布出来了。很可能这些卡在被偷走之后马上就被注销了，但警方的报告（图 6.65）罗列的个人数据信息却不是那么容易注销的。

图 6.65 警方报告的 3 起抢劫

在这起案件中，不仅受害人的驾照号码被公布了，他们的社会保险号码以及他母亲的驾照号码也都公布在了一个公开网站上，这很容易被有非法企图的人利用[1]。

社会保险号码

社会保险号码（Social Security Number, SSN）是美国公民的最重要的信息。即使没有任何经验的罪犯也能用偷来的社保号到银行开户，办各种信用卡——都用受害人的名字。本节，我们来看看个人的社保号在网上如何冻结。和本书其他敏感信息搜寻中建议相同，应采取各种措施模糊化选中的文档和用于定位它们的 Google 检索结果。

在许多教育机构里，通常都为学生分配唯一的学号，以保护学生的成绩和个人信息。然而，图 6.66 所示的学号通常使用学生的社保号码。

社保号本身不是大问题，和学生的成绩放在一起（图 6.67），系统就能为学生信息做好保密。

然而，在很多情况下，学生的名字和社保号是在一起公布的，如图 6.68 所示。这样当然破坏了匿名性，而用身份号码代替名字则不会这样。

[1] 我们显然处境不妙，因为这些搜索确实有危险性。这些与下面那些搜索信息已经被模糊处理过，任何可能被用 Google 重新搜索的信息也已经删除。另外，本章涉及的大部分敏感文件也都从网上删除了。

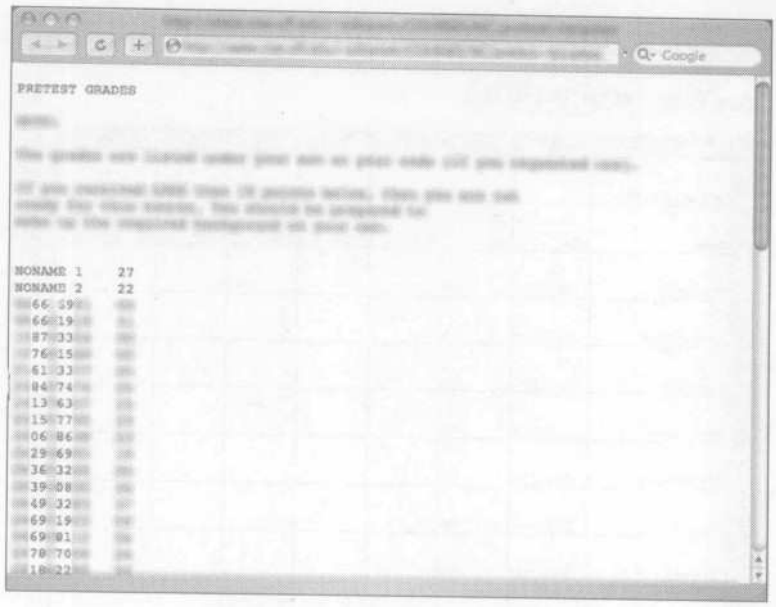


图 6.66　社保号作为学生的学号

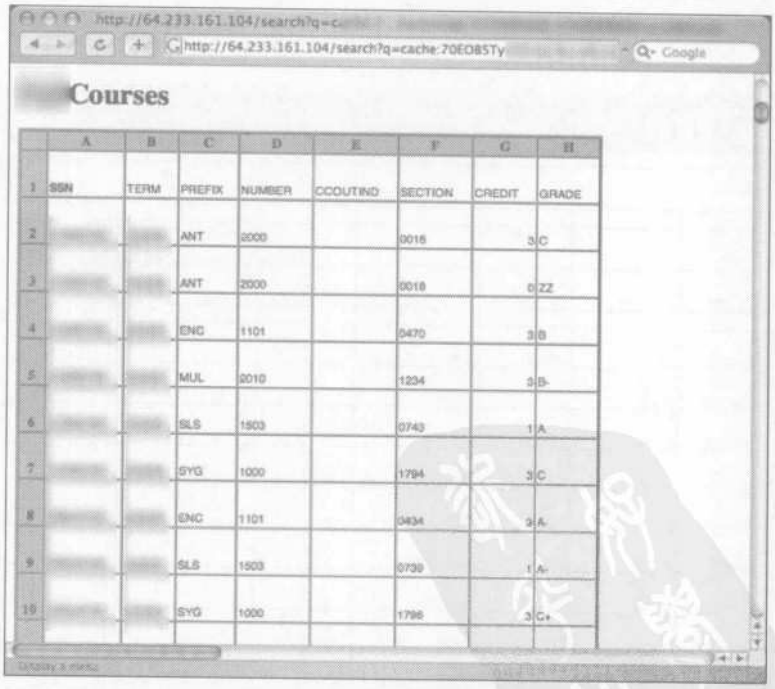


图 6.67　匿名学号和成绩单

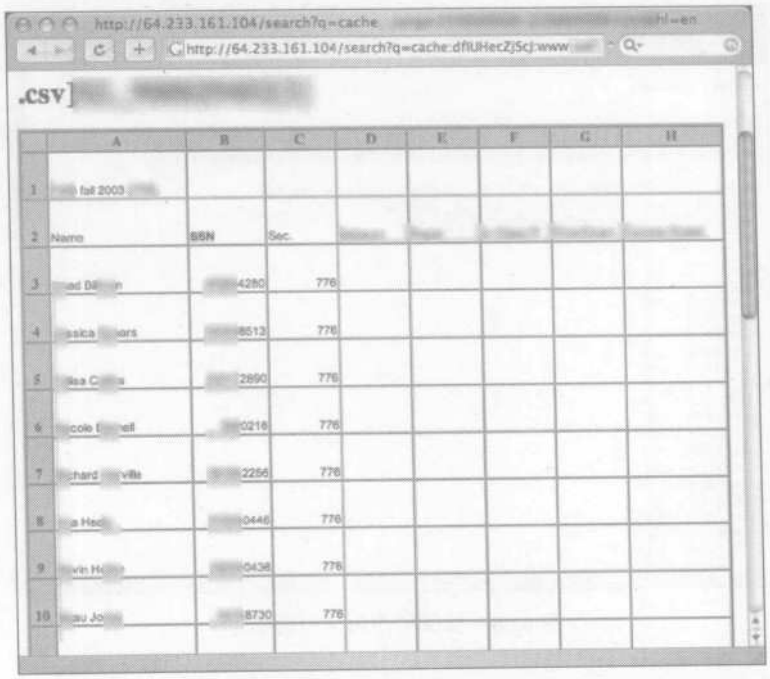


图 6.68 名字和社保号码在一起

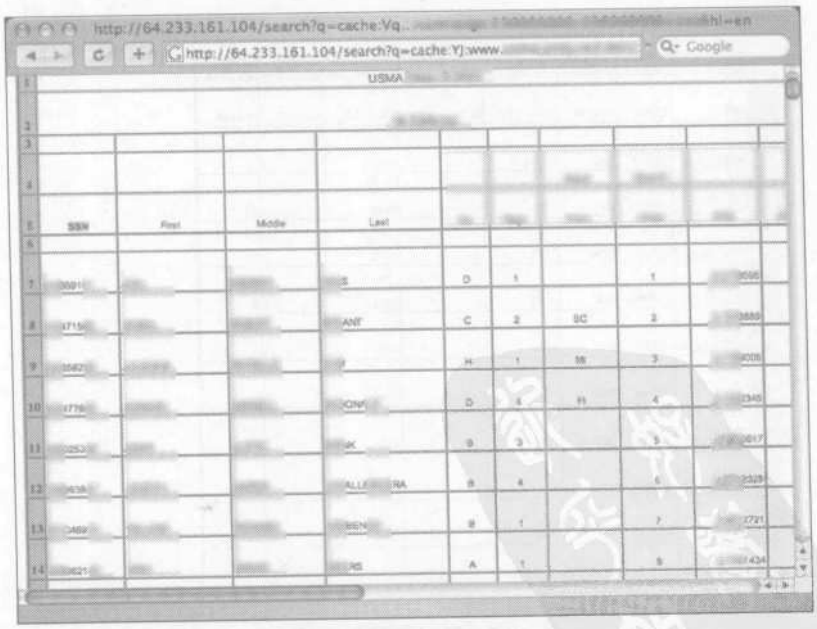


图 6.69 社保号和名字、身份证号是小偷的生日礼物

在某些情况下，这些文件是不应该公开的，但有时却出现在网络上。这当然是不安全的行为，通常这些文件会在 Google 的缓存里结束。如图 6.69 所示，是一个匿名的 Google 黑客在公开的目录里发现的。上面列出了学生的名字、社保号及其他信息。更糟的是，这个文件是在美国政府培训机构网站上发现的。现在它已经被删除了。

社会保险号码出现在网页上还有别的方式，然而最值得注意的却是用户的粗心大意。如图 6.70 所示，在申请工作的简历信息栏中列出了自己的社保号。

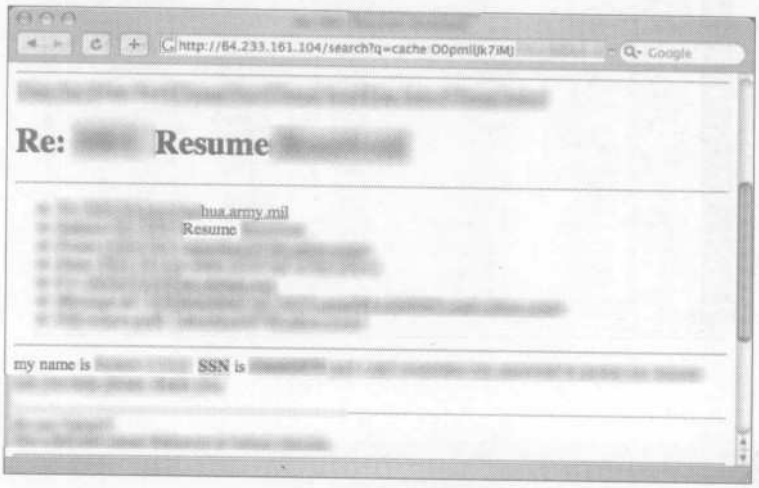


图 6.70　简历中的社保号

图 6.71 显示的文件据我所知是简历或 CV。我不确定 CV 什么含义，但研究后我发现它是一种相当聪明的简历。

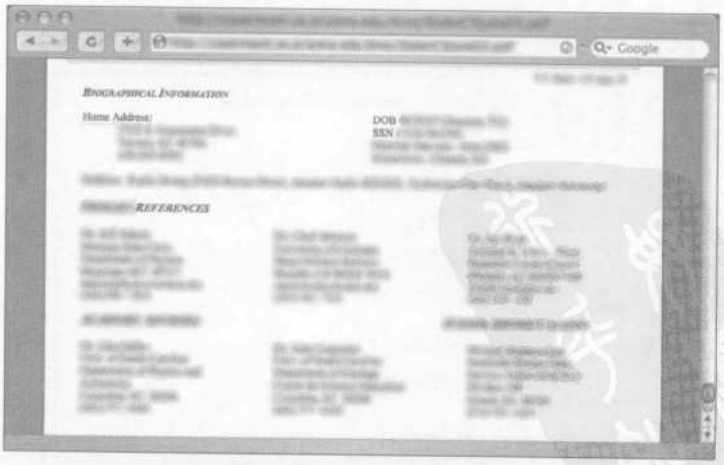


图 6.71　我很聪明，想看我的简历吗？

就个人而言，我觉得还会保留以前那种普通的简历，特别是如果使用 CV 意味着不得不公开生日和社会保险号码。最后，细心查看图 6.72 中的表格，上面列出了公司雇员的姓名、生日、性别、聘用日期、社保号等。

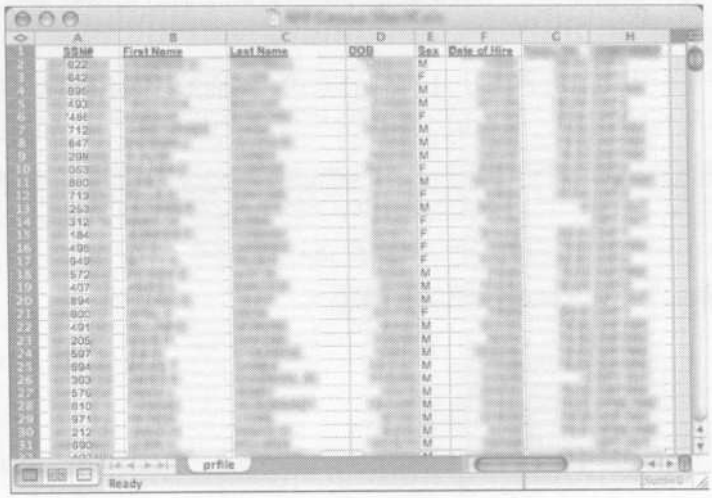


图 6.72 员工信息表

信用卡信息

信用卡号码显然很重要，需要妥善保护。然而，如本节将看到的，信用卡号可以很轻易地在网上找到。如图 6.73 所示，可以看到一个小文件里包含一个 Visa 信用卡号，还有相关的过期日期。

图 6.73 信用卡信息

从图 6.74 可以看到，一个稍大点的文件里不仅记录了信用卡号码和过期日期，还有卡的验证号码（card certification value, CVV），常被用来验证持卡人的合法身份。

图 6.74　更多信用卡信息

图 6.75　大量信用卡信息

从图 6.75 看到，一个文件里含有更多的受害者的个人信息，有名字、地址、电话号码、信用卡号、CVV 编码以及过期日期。

然而，信用卡号码和过期日期并非网上唯一的财务方面的敏感信息，如图 6.76 所示。

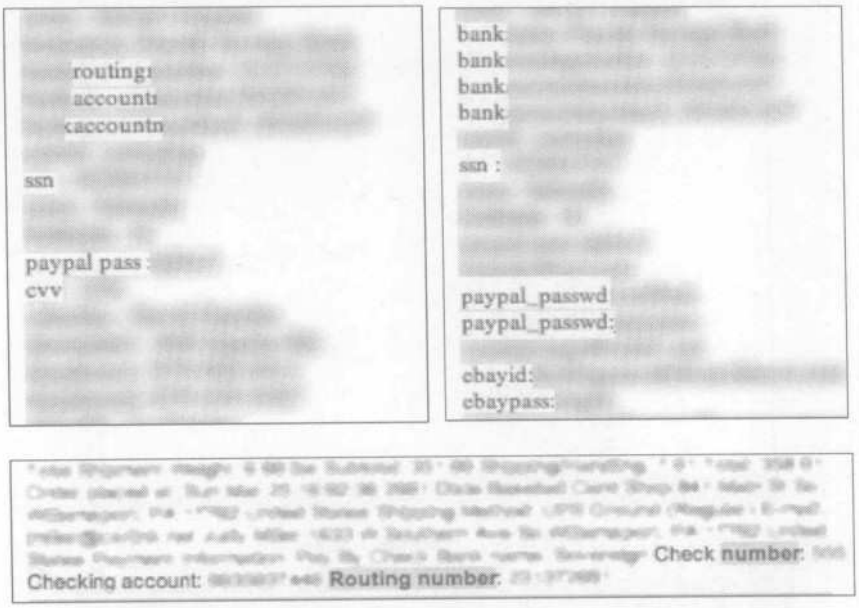


图 6.76 没什么可怕的

这些文件怎么跑到网上了呢?

通常，这种信息由飞客（利用电子通讯手段诱骗个人信息的犯罪分子）搜集，存储在网上列表或数据库中。在大多数情况下，调查人找到这些列表或数据库，再将链接传给他们，在线讨论。Google 追踪这些链接，再将捕捉到的数据透露给 Google 黑客。也有其他的情况，信用卡号交易者将数据发布到网页上公开讨论，之后这些信息被 Google 搜集并存入缓存。

这些例子来自各种类型的网站，包括银行流水号、PayPal（一种网上交易模式）的用户名和口令、eBay 用户名和口令、银行账号和流水号等，很可能被飞客弄到。

超越 Google

有时，使用 Google 搜索是黑客入侵过程的第一步。接着标准黑客会进入下一个步骤，就是脱离 Google。在这部分，我们快速看一些有趣的 Google 入侵，它们包含附加的一些步骤就可实现入侵。操作仍然很简单，这些例子展现了黑客进行的创造性改进。

第一个截屏，如图 6.77（CP 提供）所示，报道了一个员工目录出于隐私目的从网上删除。

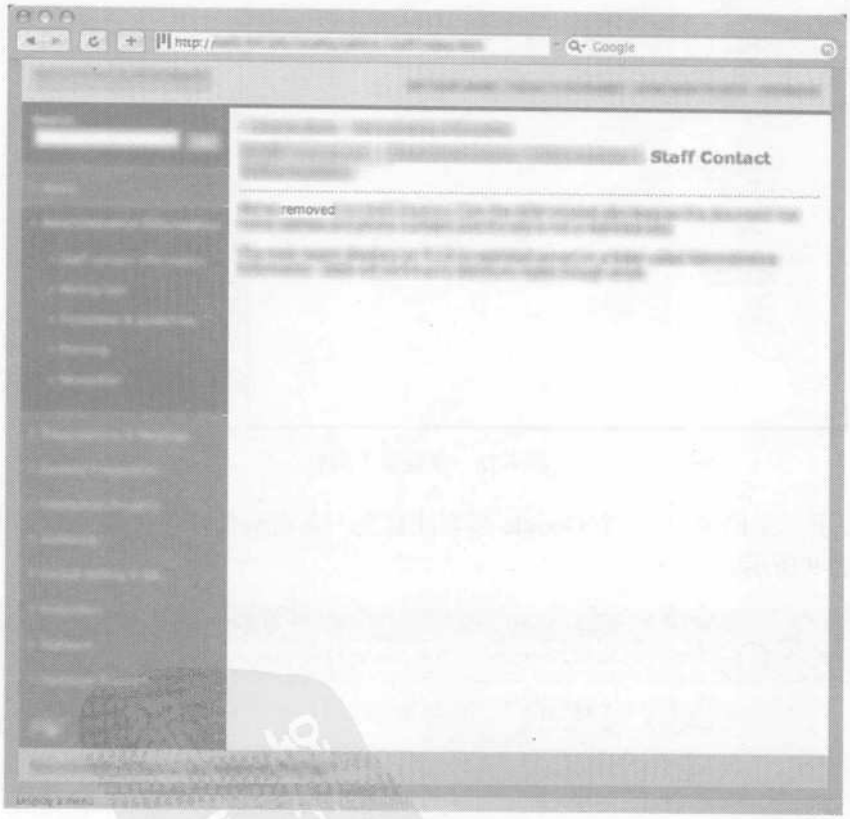


图 6.77 删除了员工列表

这个主意不错，但问题是以前的文件也必须从网站上删除，否则其他的网站如 archive.org 还将保留这些文件的链接。由图 6.78 可以看到，由于 archive.org 的链接存在，这个员工联系表还可以找出来。

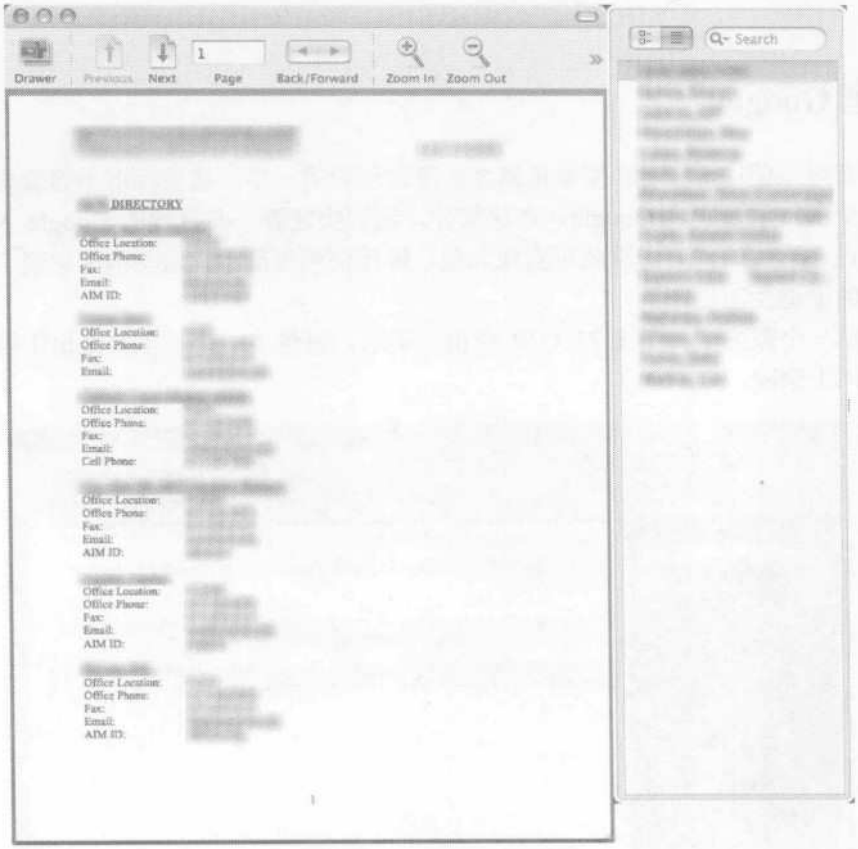


图 6.78 恢复员工列表

在下一个例子中，一个 Google 黑客注意到一条密码信息出现在 PDF 文档中，如图 6.79 所示。

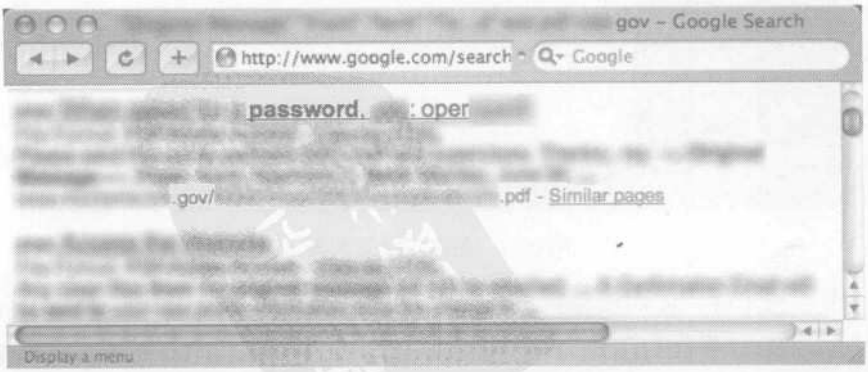


图 6.79 一个涉及密码的 PDF 文件

下载这个 PDF 文件之后发现它确实涉及密码信息。下面是这个链接，指向一个密码保护的 PDF 文件，如图 6.80 所示。

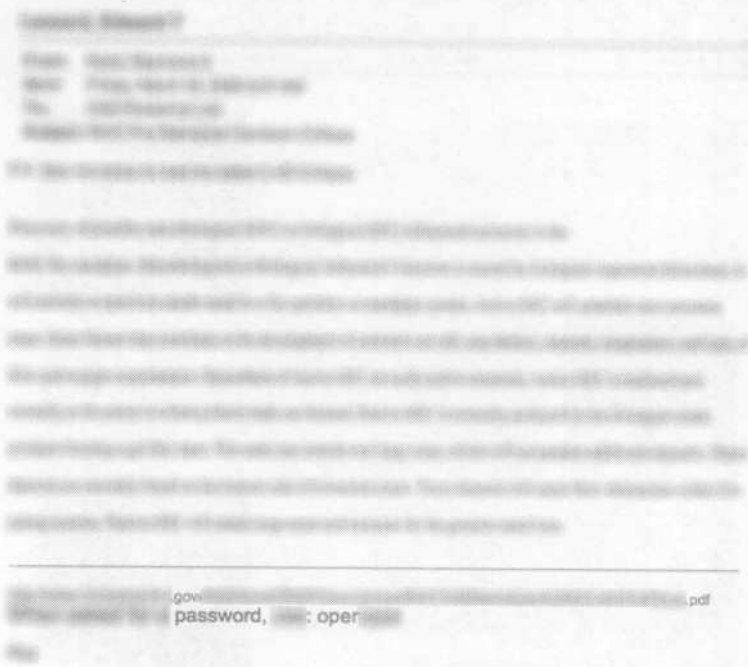


图 6.80　一个指向受密码保护文件的链接，以及相关的密码

从图 6.81 可以看到，这个 PDF 文件确实是密码保护的。

图 6.81　密码保护的 PDF 文件

输入密码打开文件，如图 6.82 所示。

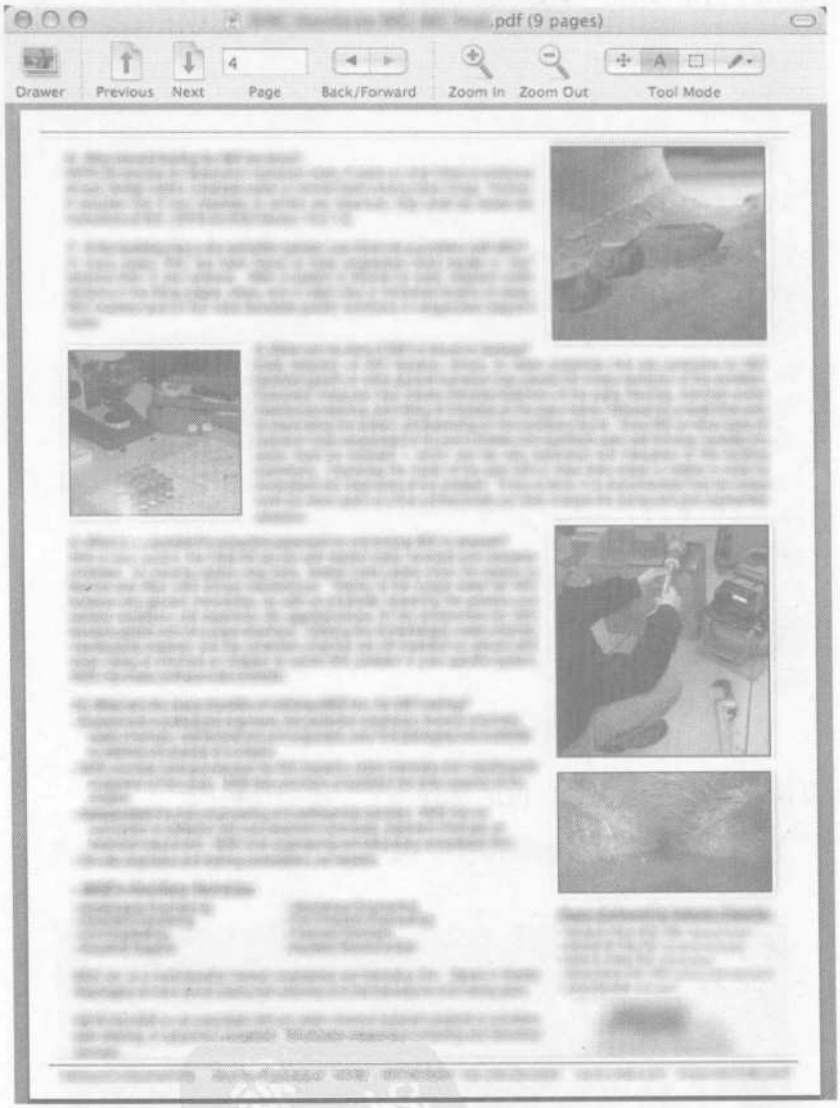
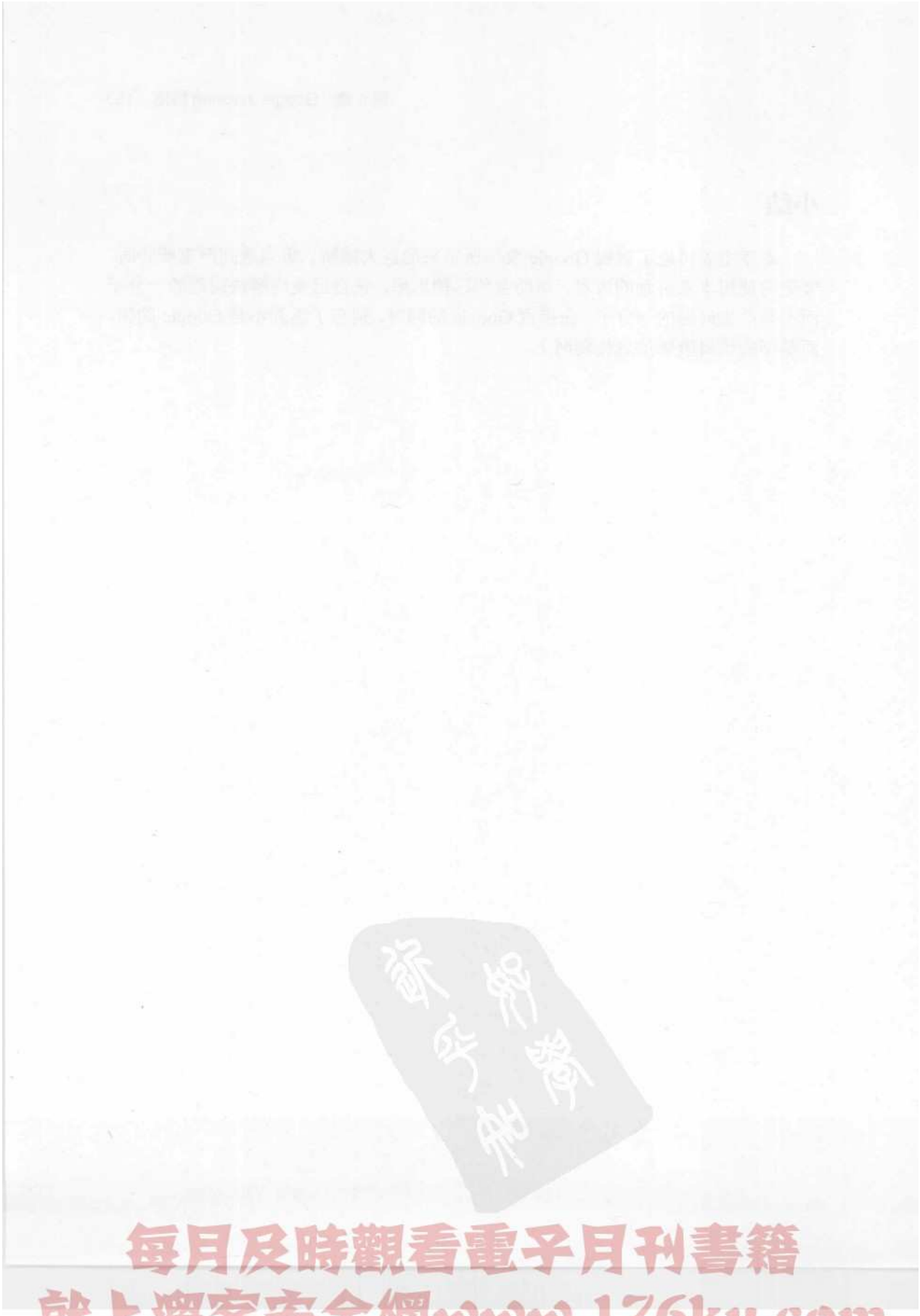


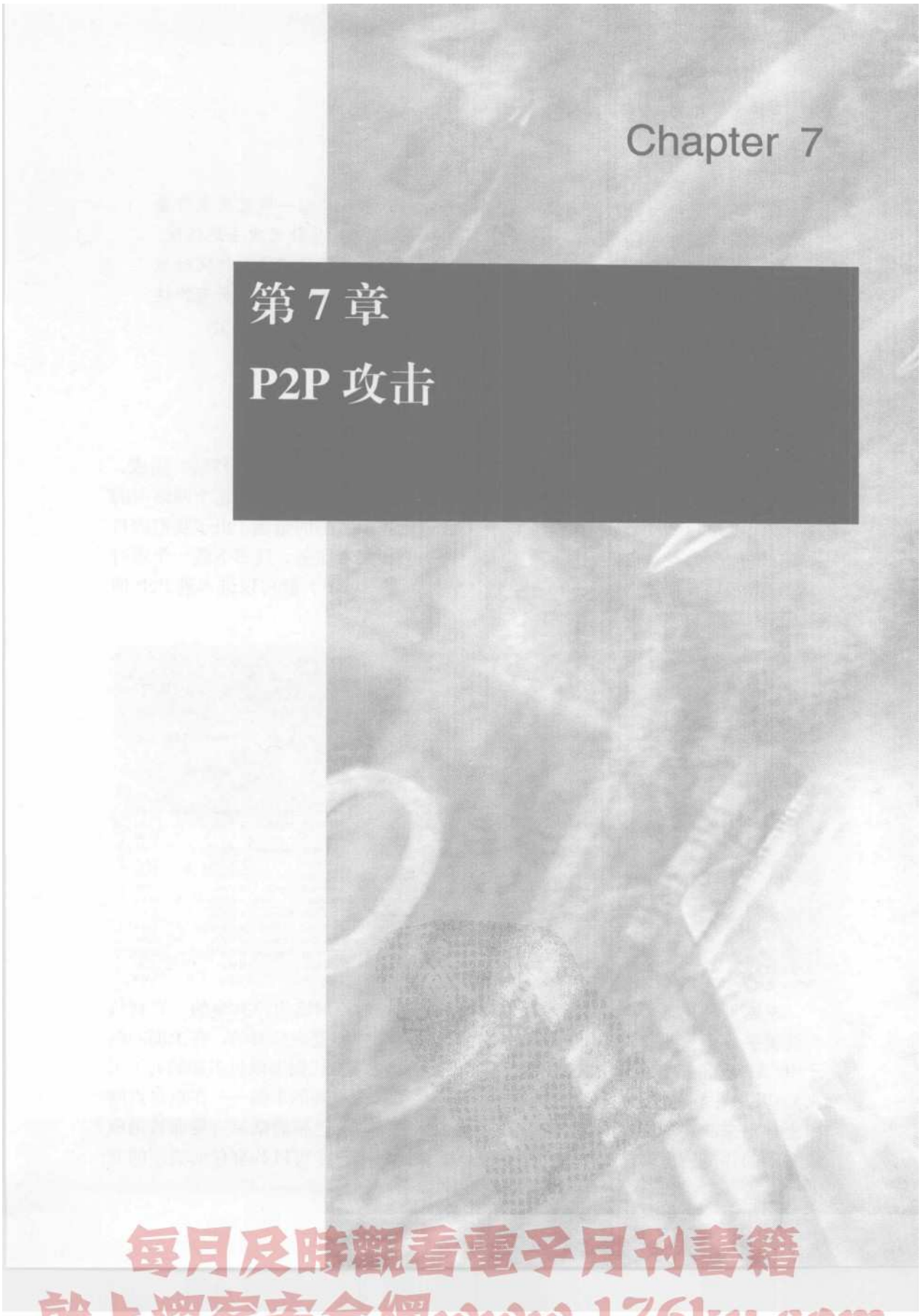
图 6.82 用盗取的密码打开敏感文件

用密码加密一个文件却又把密码公布，让人觉得多此一举，但情况通常是包含密码信息的原始文件是不公开的。不过，政府的涉密文件还是有可能泄露。

小结

本章主要讨论了忽视Google攻击所带来的巨大威胁。每当遇到严重威胁时，要记得使用本章讲到的内容。帮助宣传这种思想，使自己变成解决问题的一分子而不是产生问题的一分子。在指责Google的同时，别忘了这并不是Google的错，而是不应该将敏感信息传到网上。





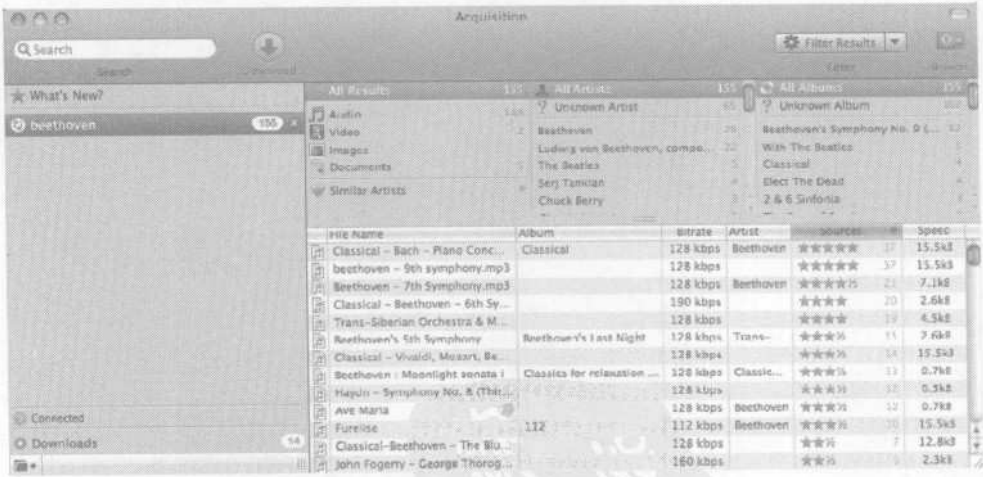
Chapter 7

第 7 章
P2P 攻击

本章暂停讨论严格意义上的非技术攻击，转而考虑一项低技术含量的攻击：点对点（pear-to-pear, P2P）攻击。这里延续非技术攻击的传统：假设一个家伙没有预算,没有商业攻击软件，没有犯罪组织的支持同时也没有任何奇特的装置。实际上，他甚至不能使用 Google。对于所有的这些限制，你认为他对你还有威胁吗？通过阅读本章来检验判断吧。

了解点对点攻击

一个点对点网络是由许多共享文档或共享数据的客户端（也叫终端）组成。通常情况下，点对点网络一般携带了音频、视频和程序文件，加入这个网络中的用户可以共享这些文件。点对点的工作方式远远超出本书的范围，出于我们的目的，让我们认为点对点网络是现实中最普通的文件共享服务。只要下载一个点对点客户端程序（如获取 Mac 的一种 P2P 软件，显示如下）就可以进入到 P2P 网络，运行它就可以开始搜索文件并进行下载。

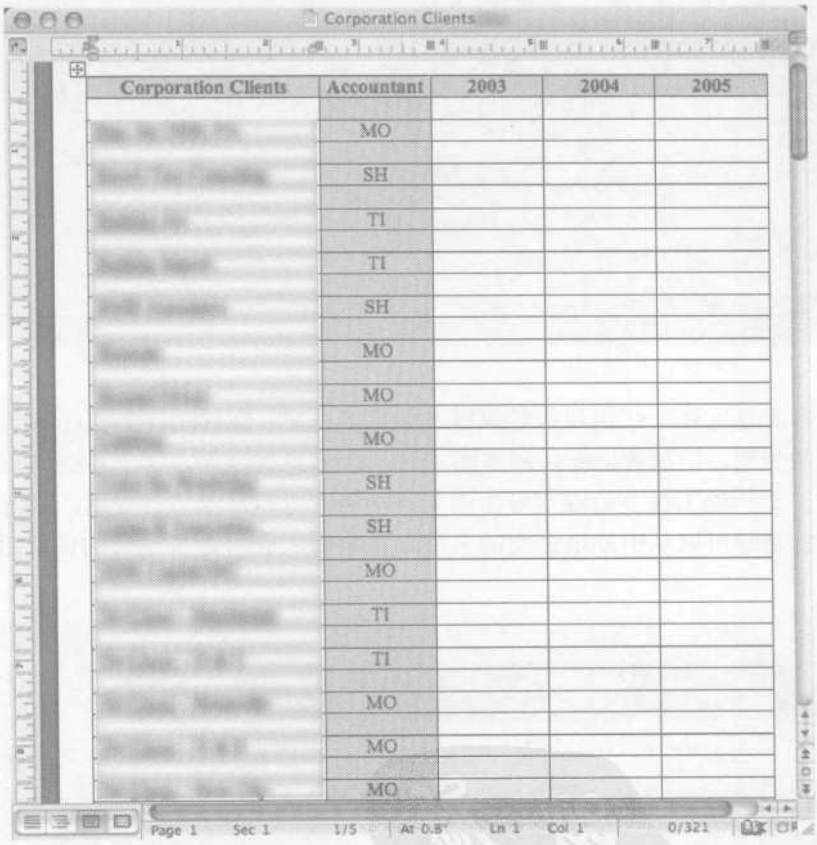


搜索贝多芬时，如上图所示我们获得了其他点对点网络用户共享的一系列包含关键字贝多芬的文件。搜索的结果主要是根据流行程度来分类的。在上面的例子中，最上面的 3 个结果包括一部巴赫的钢琴协奏曲（被错误当成贝多芬的列了出来），以及贝多芬的第七和第九交响曲。这产生了一个有趣的事情——在点对点网络上搜出来的共享文件不都是它们表面上显示的那样，巴赫的钢琴协奏曲被当成贝多芬的作品列出就是一个好例子，但是既然任何用户都可以共享任何类型的文

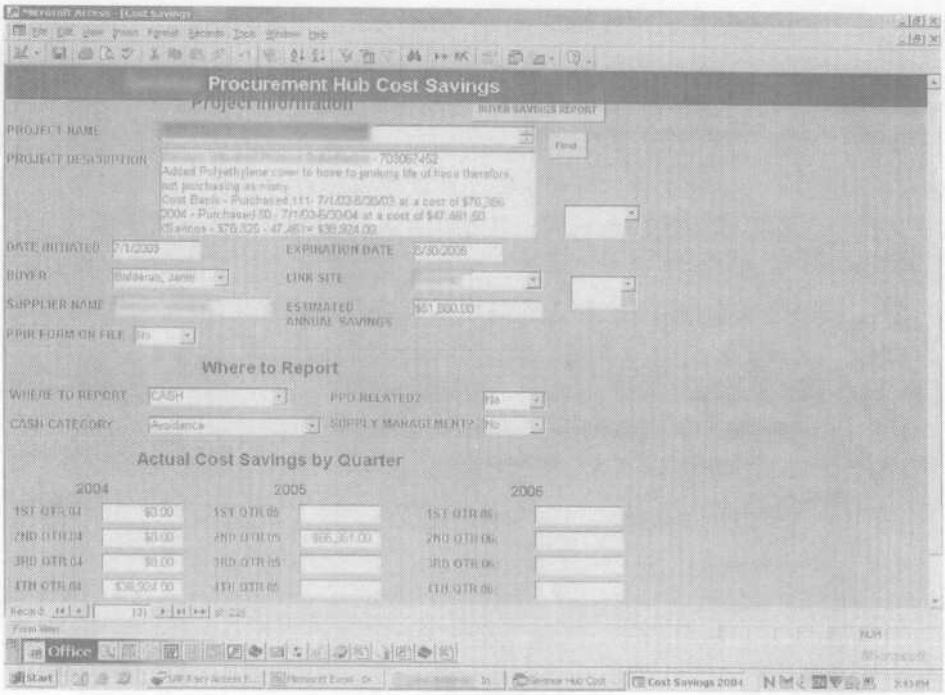
件，协奏曲也很容易是任何其他的东西：一部关于蛋黄酱的电影、一张顽皮孩子的照片、一个包含计算机病毒的文件。首先，恶意的用户可以很容易地共享任何类型的垃圾文件；其次，我对偶然地被共享的敏感文件比对恶意文件更感兴趣。

非技术黑客已经知道，有许多的因特网用户下载并安装了点对点软件，并且意外地共享了一些敏感文件。得到这些文件就像安装点对点客户端软件和提交搜索一样简单。在本章，我们将看到一些充斥在各种各样点对点网络上的文件。

我们将从基础开始并逐步延伸到一些真正有趣的东西。下面一张图片显示了一个看上去相对简单的文字文档，它列出了一个公司的所有客户。



下面这张图片的质量非常差，但我发现它时就是这样的。我想这是如扫描图片一样扫描进去的，真希望它的质量不像在报纸上打印出来的那样。

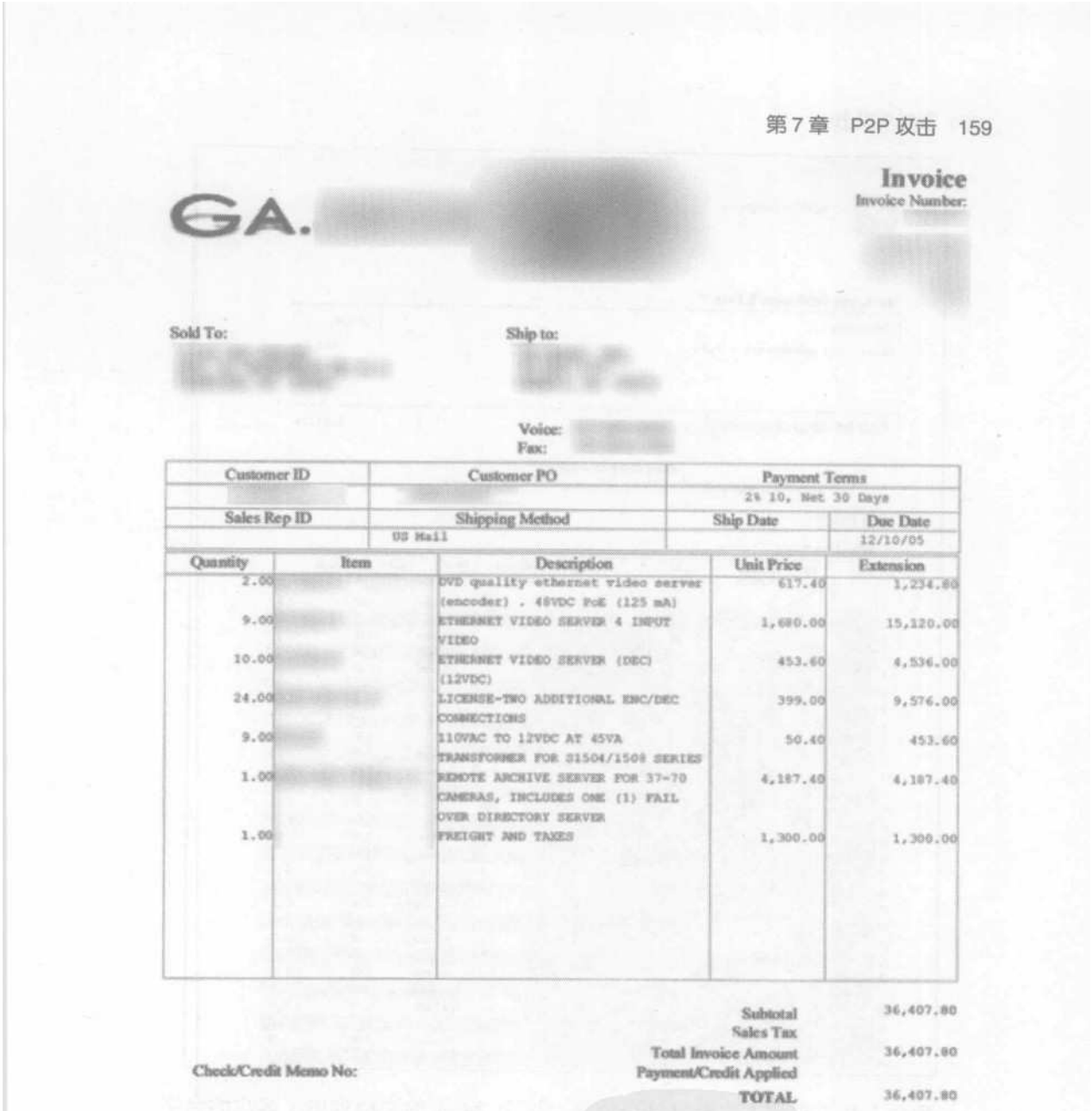


然而就是这样一张图片却能揭露非常多的信息。底部的任务栏能够实现背后偷窥者的梦想，但是数据库访问界面就是一个信息资源库。这个界面显示了一家大公司关于一项工程节约成本每个细节，包括费用和每年节省费用。这信息是陈旧的，但是却可以从中知道公司的名字，肯定有人会对更多这类的信息感兴趣。

发现一个，搜索更多

一旦发现了一个有趣的文档，从同一部计算机里，可以很简单地发现更多。大部分点对点客户允许浏览在计算机上的所有共享文件。如果一个攻击者发现一个敏感的文档，他将几乎肯定可以通过浏览那台共享的计算机发现更多信息。虽然搜索仅仅局限于共享的文件，但是如果用户共享了一个敏感的文档，几乎肯定共享了其他的敏感文件。

下面的图片显示了一张顾客的发票。



GA.

Invoice
Invoice Number:

Sold To:

Ship to:

Voice:
Fax:

Customer ID	Customer PO	Payment Terms	
		2% 10, Net 30 Days	
Sales Rep ID	**Shipping Method**	**Ship Date**	**Due Date**
	US Mail		12/10/05

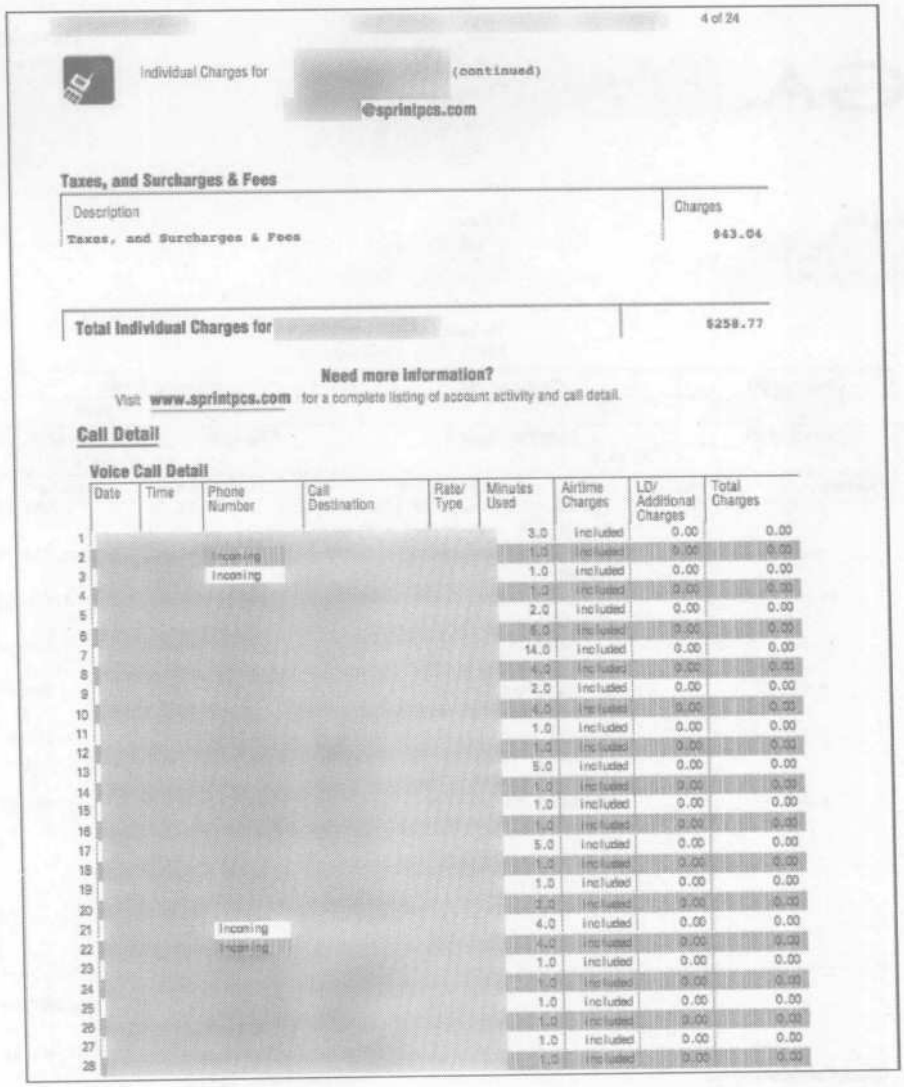
Quantity	Item	Description	Unit Price	Extension
2.00		DVD quality ethernet video server (encoder) . 48VDC PoE (125 mA)	617.40	1,234.80
9.00		ETHERNET VIDEO SERVER 4 INPUT VIDEO	1,680.00	15,120.00
10.00		ETHERNET VIDEO SERVER (DEC) (12VDC)	453.60	4,536.00
24.00		LICENSE-TWO ADDITIONAL ENC/DEC CONNECTIONS	399.00	9,576.00
9.00		110VAC TO 12VDC AT 45VA TRANSFORMER FOR 31504/1508 SERIES	50.40	453.60
1.00		REMOTE ARCHIVE SERVER FOR 37-70 CAMERAS, INCLUDES ONE (1) FAIL OVER DIRECTORY SERVER	4,187.40	4,187.40
1.00		FREIGHT AND TAXES	1,300.00	1,300.00

Subtotal	36,407.80
Sales Tax	
Total Invoice Amount	36,407.80
Payment/Credit Applied	
TOTAL	36,407.80

Check/Credit Memo No:

这张发票也是过期的，但是显示了客户的信息和价格数据。我最感兴趣的是发票列出的项目描述，它包含了一个非常高端的安全系统。它列出了视频服务器（相当于 40 部照相机的容量）、视频编码器、电源供应等。这张关于一个高科技安全系统的发票会出现在一个让世界上所有人都能见到的 P2P 网络上简直是个笑话。

下面是另一个有趣的文档：一张手机账单。



4 of 24

Individual Charges for [redacted] (continued)

[redacted]@sprintpcs.com

Taxes, and Surcharges & Fees

Description	Charges
Taxes, and Surcharges & Fees	943.04

Total Individual Charges for [redacted] **$258.77**

Need more information?

Visit **www.sprintpcs.com** for a complete listing of account activity and call detail.

Call Detail

Voice Call Detail

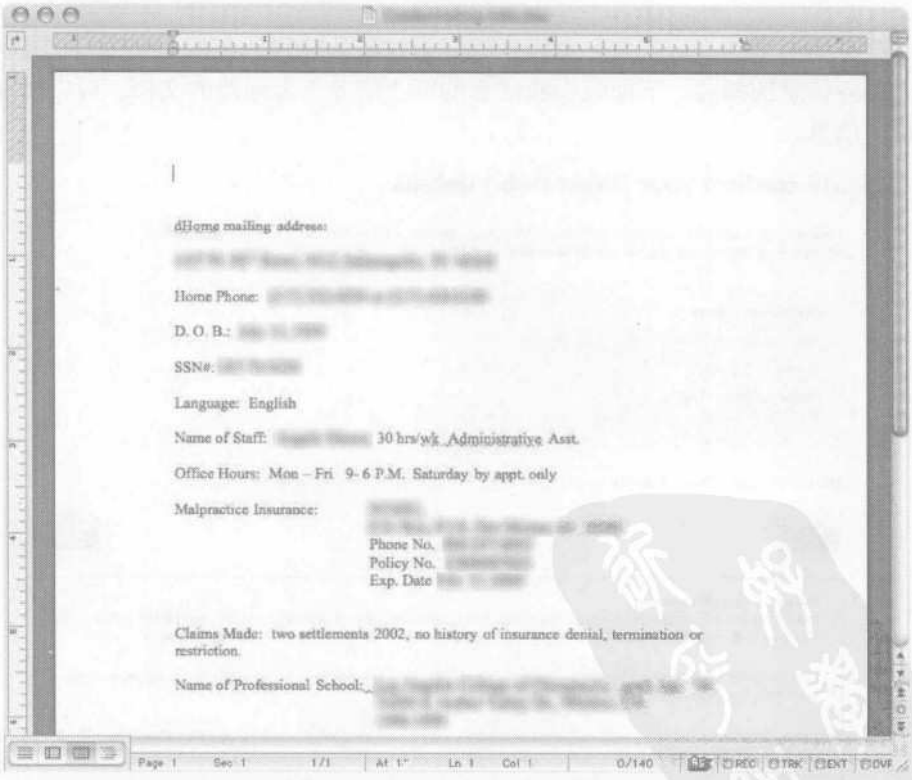
	Date	Time	Phone Number	Call Destination	Rate/ Type	Minutes Used	Airtime Charges	LD/ Additional Charges	Total Charges
1	[redacted]					3.0	Included	0.00	0.00
2				Incoming		1.0	Included	0.00	0.00
3				Incoming		1.0	Included	0.00	0.00
4						1.0	Included	0.00	0.00
5						2.0	Included	0.00	0.00
6						6.0	Included	0.00	0.00
7						14.0	Included	0.00	0.00
8						4.0	Included	0.00	0.00
9						2.0	Included	0.00	0.00
10						4.0	Included	0.00	0.00
11						1.0	Included	0.00	0.00
12						1.0	Included	0.00	0.00
13						5.0	Included	0.00	0.00
14						1.0	Included	0.00	0.00
15						1.0	Included	0.00	0.00
16						1.0	Included	0.00	0.00
17						5.0	Included	0.00	0.00
18						1.0	Included	0.00	0.00
19						1.0	Included	0.00	0.00
20						2.0	Included	0.00	0.00
21				Incoming		4.0	Included	0.00	0.00
22				Incoming		4.0	Included	0.00	0.00
23						1.0	Included	0.00	0.00
24						1.0	Included	0.00	0.00
25						1.0	Included	0.00	0.00
26						1.0	Included	0.00	0.00
27						1.0	Included	0.00	0.00
28						1.0	Included	0.00	0.00

我个人并不想和大家分享这个信息。这个 24 页的文档列出了客户的名字、住址和电话号码，而且列出了整个月的详细通话记录。它列出了每个拨入和拨出的电话，还列出了时间、通话时间和每月的费用。如果一个高技术黑客试着得到这一笔电子数据，那会是一件非常困难的工作。但是对一个非技术黑客而言，这仅仅需要一次快速的点对点攻击或一次“垃圾箱潜伏”（指在垃圾箱中寻找有价值的东西）。

如果黑客在寻找我呢?

一想到黑客的攻击目标是个人信息就让人觉得可怕，但点对点攻击的目标不是特定的个人信息。点对点攻击是为了发现以特定关键字为基础的有趣的信息。如果一个黑客盯上你了，他可能不会运行点对点客户程序搜索你，因为这需要假设你运行点对点客户端，并且你共享了个人数据。这两个假设都是相当疯狂的。因此如果的确在运行点对点软件，一定要确保知道正在共享什么且注意个人防火墙、防病毒/反间谍/入侵检测软件均配置正确，并正在使用。

文本文档充满了点对点网络，包含了大量的个人信息。下面的文档列出的信息比大部分文档中包含的个人信息要多。



名字、出生日期和社会保险号码是一些有趣的数据，但是这份文件也揭露了保险单数据。与财务数据相比，这些都显得苍白。让我们看下面的文档。

Attach your Schedule 1 (federal tax), and Form 428 (provincial or territorial tax) here. Also attach here any other schedules, information slips, forms, receipts, and documents that you need to include with your return.

Net income

Enter your **total income** from line 150			150	53,331	40
Pension adjustment (box 52 on T4, box 34 on all T4A slips)	206	1,396 00			
Registered pension plan deduction (box 20 on all T4 slips and box 32 on all T4A slips)			207	550	36
RRSP deduction (see Schedule 7; attach receipts)			208	1,420	76
Saskatchewan Pension Plan deduction		(maximum $600)	209		
Annual union, professional, or like dues (box 44 on all T4 slips and receipts)			212	950	90
Child care expenses (attach Form T778)			214		
Attendant care expenses			215		
Business investment loss Gross 228		Allowable deduction	217		
Moving expenses			219		
Support payments made Total 230		Allowable deduction	220		
Carrying charges and interest expenses (attach Schedule 4)			221		
Deduction for CPP or QPP contributions on self-employment and other earnings (attach Schedule 8)			222		•
Exploration and development expenses (attach Form T1229)			224		
Other employment expenses			229		
Clergy residence deduction			231		
Other deductions. Specify:			232		
Add lines 207 to 224, 229, 231, and 232			233	2,922	04
					2,922 04
Line 150 minus line 233. This is your **net income before adjustments.**			234		50,409 38
Social benefits repayment (if you reported income on line 113, 119, or 146, see Help)			235		•
Line 234 minus line 235 (if negative, enter "0"). If you have a spouse or common-law partner, **see Help.** This is your **net income.**			236		50,409 38

这份纳税文件很可能是一个以计算机为基础的纳税计划的一部分。它提供了私人财务信息的摘要。下面吸引我注意的以“借方”为标题的文档，可以发现更多财务信息。

Please confirm your Direct Debit details

Please confirm that your payment details are correct, then place your order. If you've made any errors when typing in your information, you can still go back and correct them.

Direct Debit Details:

Name of account holder:

Branch Sort Code:

Bank / building society account number:

The company name that will appear on your bank statement against the direct debit will be Wanadoo.

Back Next

The Direct Debit Guarantee:

The Direct Debit Guarantee is offered by all banks and building societies that take part in the Direct Debit scheme. The efficiency and security of the scheme is monitored and protected by your own bank or building society.

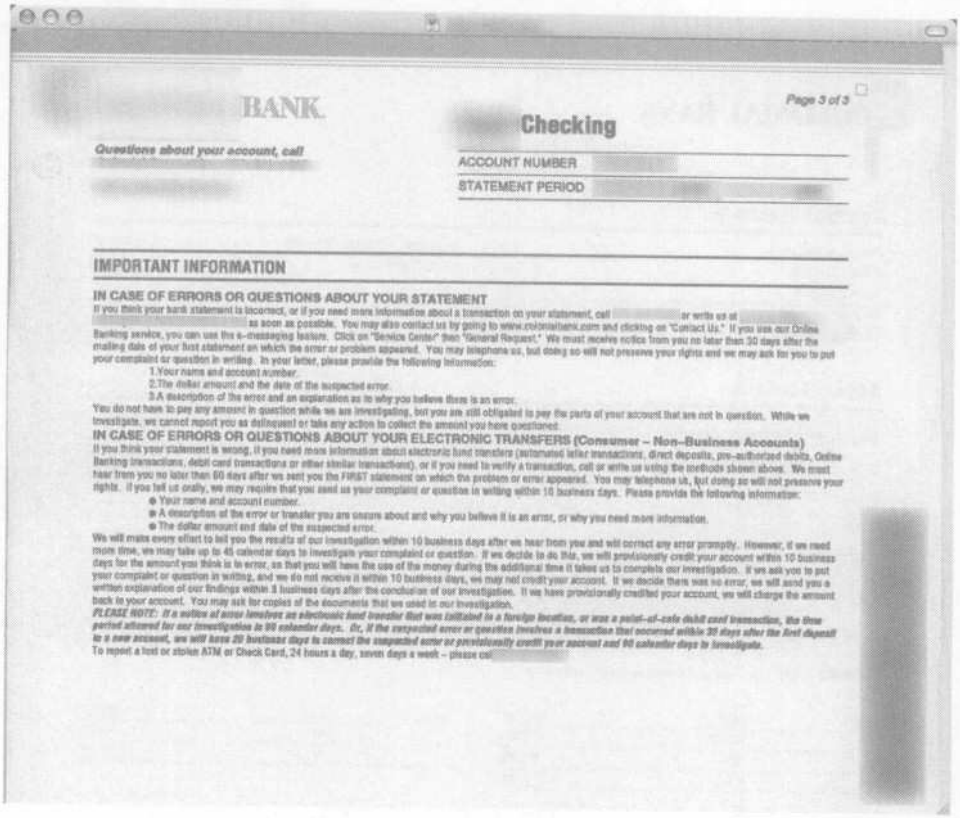
If the amounts to be paid or if the payment dates change Wanadoo will notify you 10 working days in advance of your account being debited or as otherwise agreed.

If an error is made by [redacted] or your bank or building society, you are guaranteed a full and immediate refund from your branch of the amount paid.

You can cancel a Direct Debit at any time by writing to your bank or building society. Please also send a copy of your letter to us.

这个文档的拥有者在浏览器中首先看到它，然后可能把它保存在当地的硬盘里。不幸的是，它保存在一个目录里，而点对点软件正把这个目录当作一个共享文件夹，然后这个文档就被所有人都共享了。他的名字、银行账号和部门密码如今成为了公开的内容。

其他的银行信息也容易通过如下一张照片获得。



BANK

Page 3 of 3

Checking

Questions about your account, call

ACCOUNT NUMBER

STATEMENT PERIOD

IMPORTANT INFORMATION

IN CASE OF ERRORS OR QUESTIONS ABOUT YOUR STATEMENT

If you think your bank statement is incorrect, or if you need more information about a transaction on your statement, call or write us at as soon as possible. You may also contact us by going to www.colonialbank.com and clicking on "Contact Us." If you use our Online Banking service, you can use its e-messaging feature. Click on "Service Center" then "General Request." We must receive notice from you no later than 30 days after the mailing date of your first statement on which the error or problem appeared. You may telephone us, but doing so will not preserve your rights and we may ask for you to put your complaint or question in writing. In your letter, please provide the following information:

1.Your name and account number.
2.The dollar amount and the date of the suspected error.
3.A description of the error and an explanation as to why you believe there is an error.

You do not have to pay any amount in question while we are investigating, but you are still obligated to pay the parts of your account that are not in question. While we investigate, we cannot report you as delinquent or take any action to collect the amount you have questioned.

IN CASE OF ERRORS OR QUESTIONS ABOUT YOUR ELECTRONIC TRANSFERS (Consumer – Non-Business Accounts)

If you think your statement is wrong, if you need more information about electronic fund transfers (automated teller transactions, direct deposits, pre-authorized debits, Online Banking transactions, debit card transactions or other similar transactions), or if you need to verify a transaction, call or write us using the methods shown above. We must hear from you no later than 60 days after we sent you the FIRST statement on which the problem or error appeared. You may telephone us, but doing so will not preserve your rights. If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days. Please provide the following information:

- Your name and account number.
- A description of the error or transfer you are unsure about and why you believe it is an error, or why you need more information.
- The dollar amount and date of the suspected error.

We will make every effort to tell you the results of our investigation within 10 business days after we hear from you and will correct any error promptly. However, if we need more time, we may take up to 45 calendar days to investigate your complaint or question. If we decide to do this, we will provisionally credit your account within 10 business days for the amount you think is in error, so that you will have the use of the money during the additional time it takes us to complete our investigation. If we ask you to put your complaint or question in writing, and we do not receive it within 10 business days, we may not credit your account. If we decide there was no error, we will send you a written explanation of our findings within 3 business days after the conclusion of our investigation. If we have provisionally credited your account, we will charge the amount back in your account. You may ask for copies of the documents that we used in our investigation.

PLEASE NOTE: If a notice of error involves an electronic fund transfer that was initiated in a foreign location, or was a point-of-sale debit card transaction, the time period allowed for our investigation is 90 calendar days. Or, if the suspected error or question involves a transaction that occurred within 30 days after the first deposit to a new account, we will have 20 business days to correct the suspected error or provisionally credit your account and 90 calendar days to investigate.

To report a lost or stolen ATM or Check Card, 24 hours a day, seven days a week – please call

这份多页文件列出了账目信息，包括账号数据、收支差额、费用和回收。在文件的最后包括如下图所示的报告。

BANK

Page 1 of 3

Checking

Questions about your account, call

ACCOUNT NUMBER

STATEMENT PERIOD

Bank appreciates your business. Thank you for being our Customer.

Account Summary

Previous Balance	$ 0.00	Average Collected Balance	$ 248.20
Total Credit(s)	+ 798.97	Fees This Period	$ 0.00
Total Debit(s)	- 722.36		
Service Charge	- 0.00		
Ending Balance	$ 76.61		

Account Details

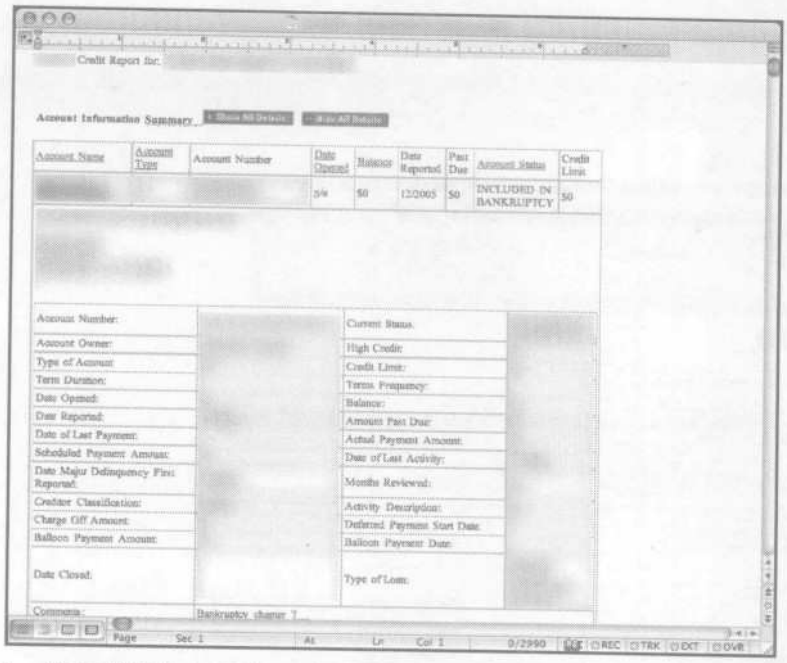
Deposits and Other Credits

DATE	DESCRIPTION	AMOUNT
12/27	DEPOSIT	50.00
12/27	DEPOSIT	700.00
12/29		0.00
1/11		0.84
1/18		48.13

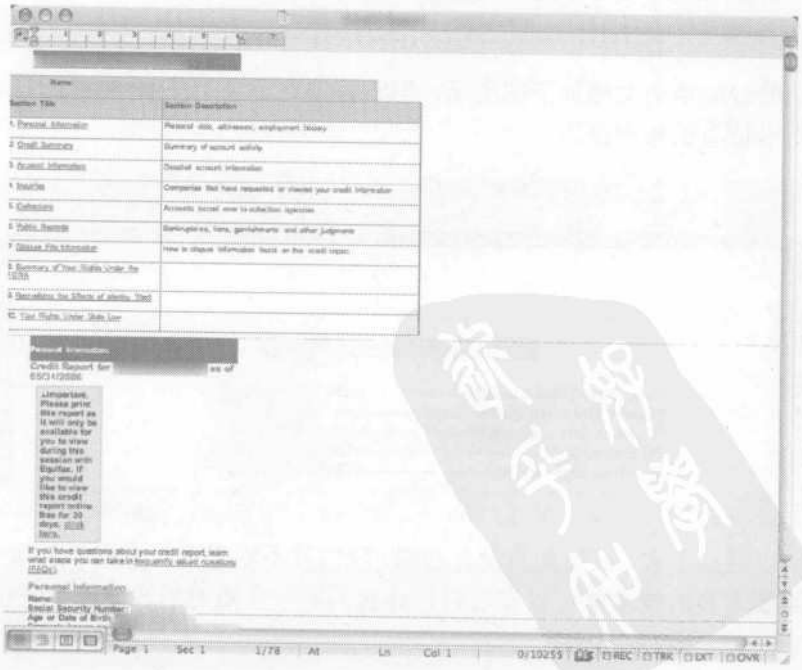
Checks Paid ▲ *indicates check missing in sequence*

CHECK	DATE	AMOUNT	CHECK	DATE	AMOUNT
	12/30	128.83		1/13	75.30
	1/3	66.96		1/13	189.29
	1/5	213.85			

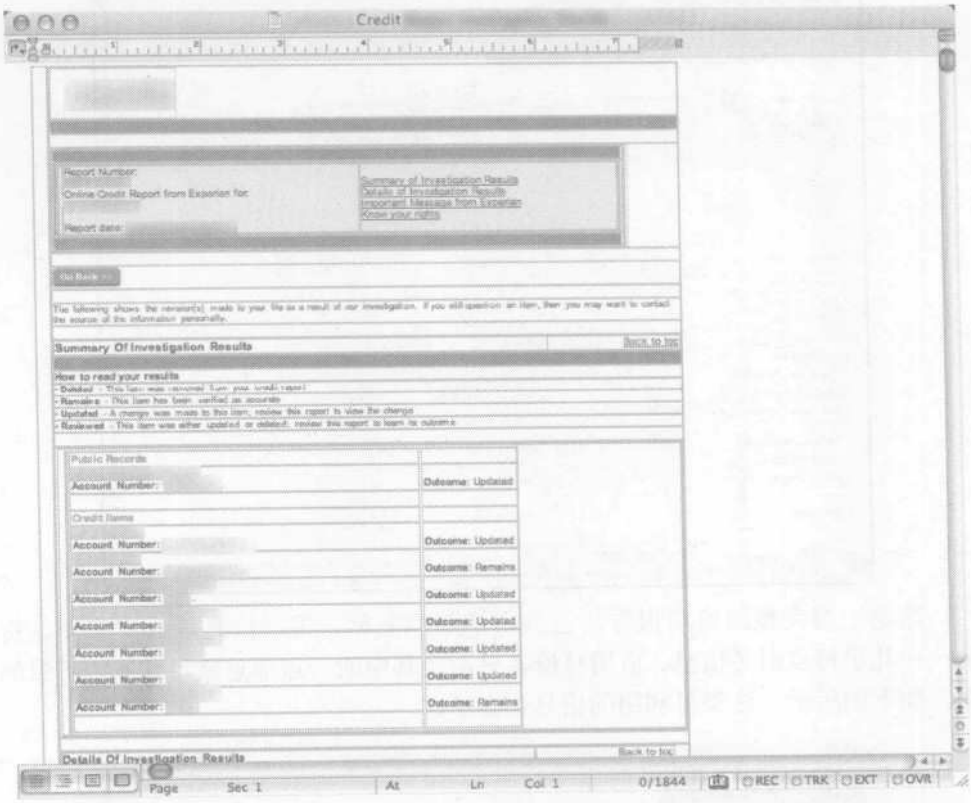
对于一个非技术黑客来说，这是一个非常好的东西，但只描述了一个单一的账户。下面的文档列出了多个账目信息，现在我们将得到一些真正令人疯狂的材料了。



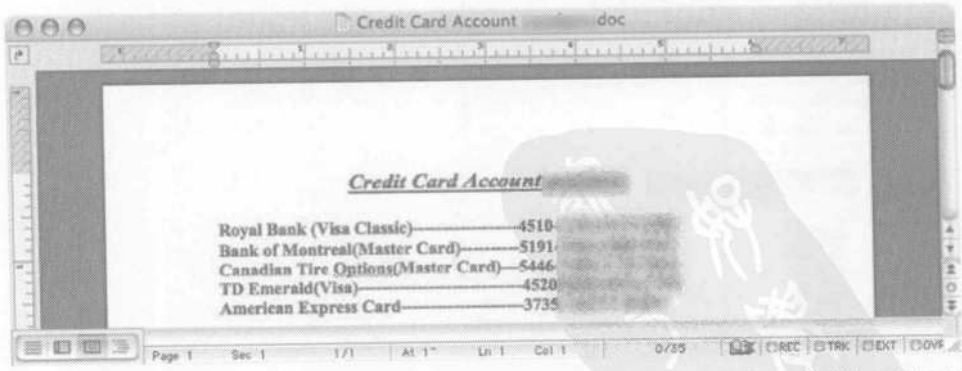
这是一篇完整的信用报告。它列出了账户名称、银行信息、收支差额、贷款……几乎每点财务信息。盗用身份者只需要其中的一点信息就足够了。不幸的是，如下图所示，这类可利用的信息更多了。



我可以举出很多这样的例子，再来看一个。



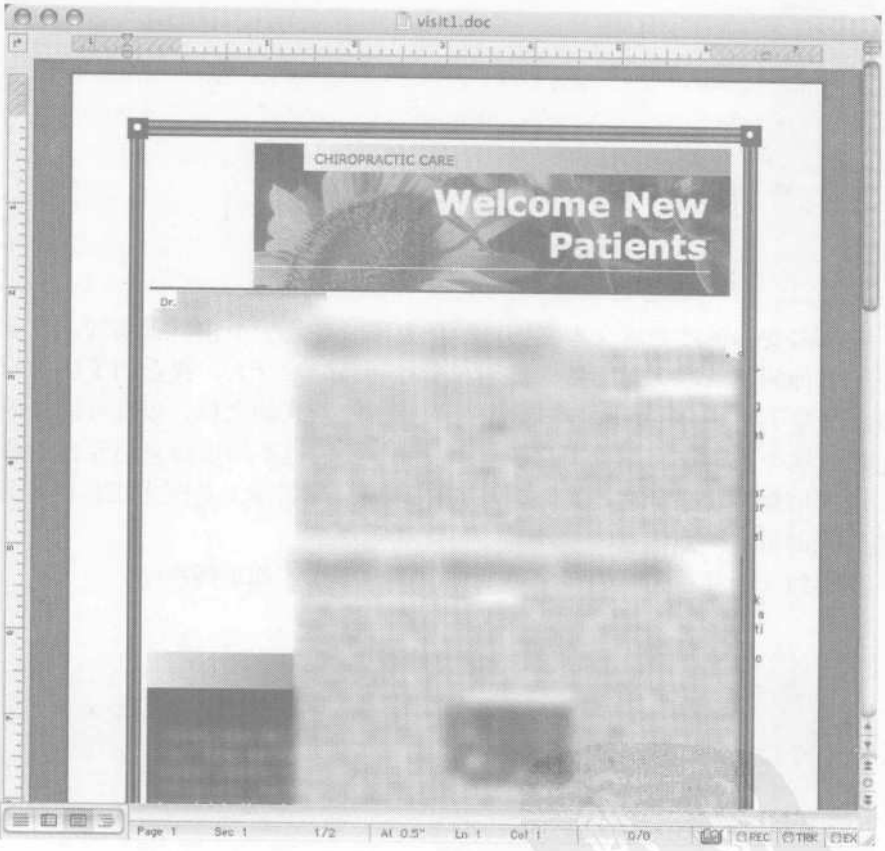
其他的较简单的文档如下图所示，但它偏偏列出了一些敏感的信息，就像是一个信用卡信息的集中报告。



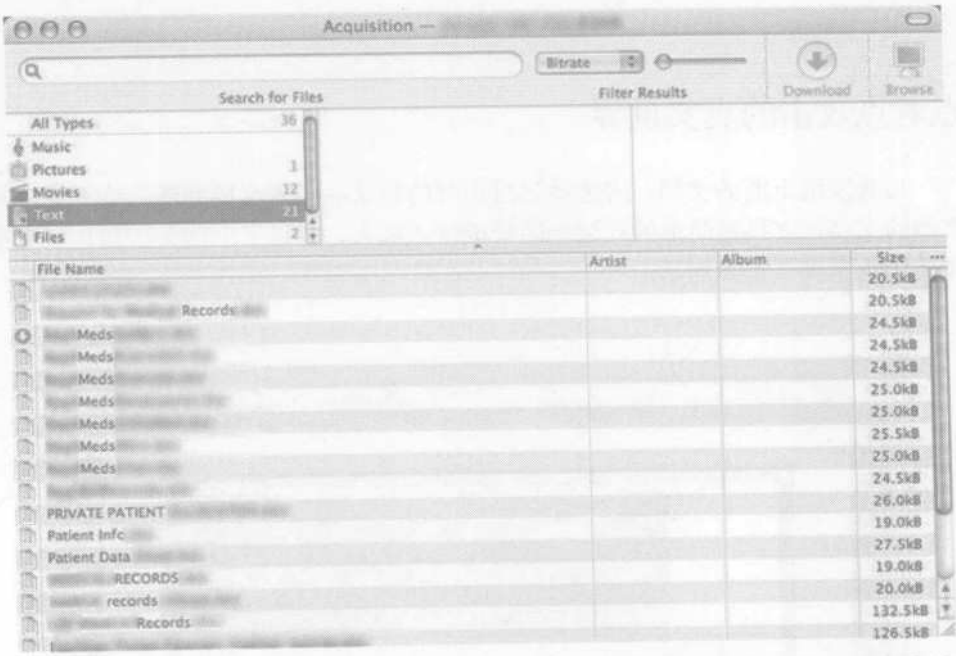
我可以继续下去，但是真的没有必要。我们并不缺乏点对点网络的敏感信息，并且不需要太多的技术就可以发现它。让我们看一个点对点攻击的真正情况吧。

点对点攻击的真实世界

当我发现下面的文档，清楚地记得那时的想法——多么聪明呀。这不是一篇有趣的文档，它只是简单的欢迎新的脊椎矫正病人，并说了一些关于肌肉、脊椎和装填物是多么重要的话。

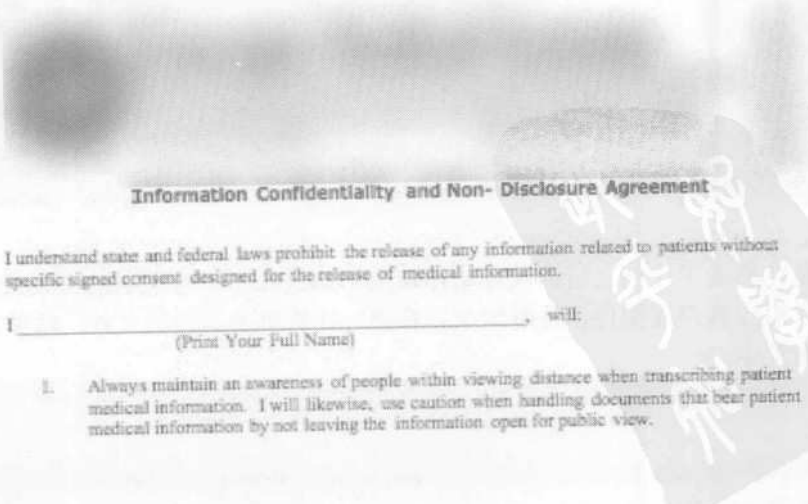


但是在思考了片刻之后，我开始怀疑是不是进入了一台医生的个人计算机。我右击点对点客户端文件，并用浏览器看那台计算机的其他的文件。结果显示在下一张图片中。



我单击文本链接查看文本文档，拉下菜单时，几乎不相信看到的。我看到了一份份文件的记录、病人的私人数据和药方（药物治疗）。我看到了病人的私人数据，浏览了一些有关病人药方数据等极其敏感信息的文件，极有可能其他一些人已经在这个点对点网络上下载了这些文档。我们也不知道信息已经传到哪里去了。这些信息使我感觉这不是一台私人计算机，这基本上是医生工作的计算机。我决定再浏览多一点信息。

我看到一个并不起眼的名字的文件，下载下来，如下图所示。



Information Confidentiality and Non- Disclosure Agreement

I understand state and federal laws prohibit the release of any information related to patients without specific signed consent designed for the release of medical information.

I _____, will:
(Print Your Full Name)

1. Always maintain an awareness of people within viewing distance when transcribing patient medical information. I will likewise, use caution when handling documents that bear patient medical information by not leaving the information open for public view.

2. Disclose this information solely to individuals who have signed a non-disclosure agreement with, or who have expressed written approval from [redacted] to receive information.

3. Not make any contact nor agreement with anyone without written and/or verbal consent from [redacted] or its authorized staff on any idea submitted without approval.

4. I agree not to use, directly or indirectly, any such information provided by [redacted] for my own benefit of any person, firm, or corporation.

5. All subcontractors and affiliates of this company have a moral, professional and legal obligation to protect the confidentiality of patient, physician, employee and administrative information. It is the obligation of the employee/subcontractor to maintain confidentiality while on and off duty. This obligation continues even after the termination of the employment relationship has ended.

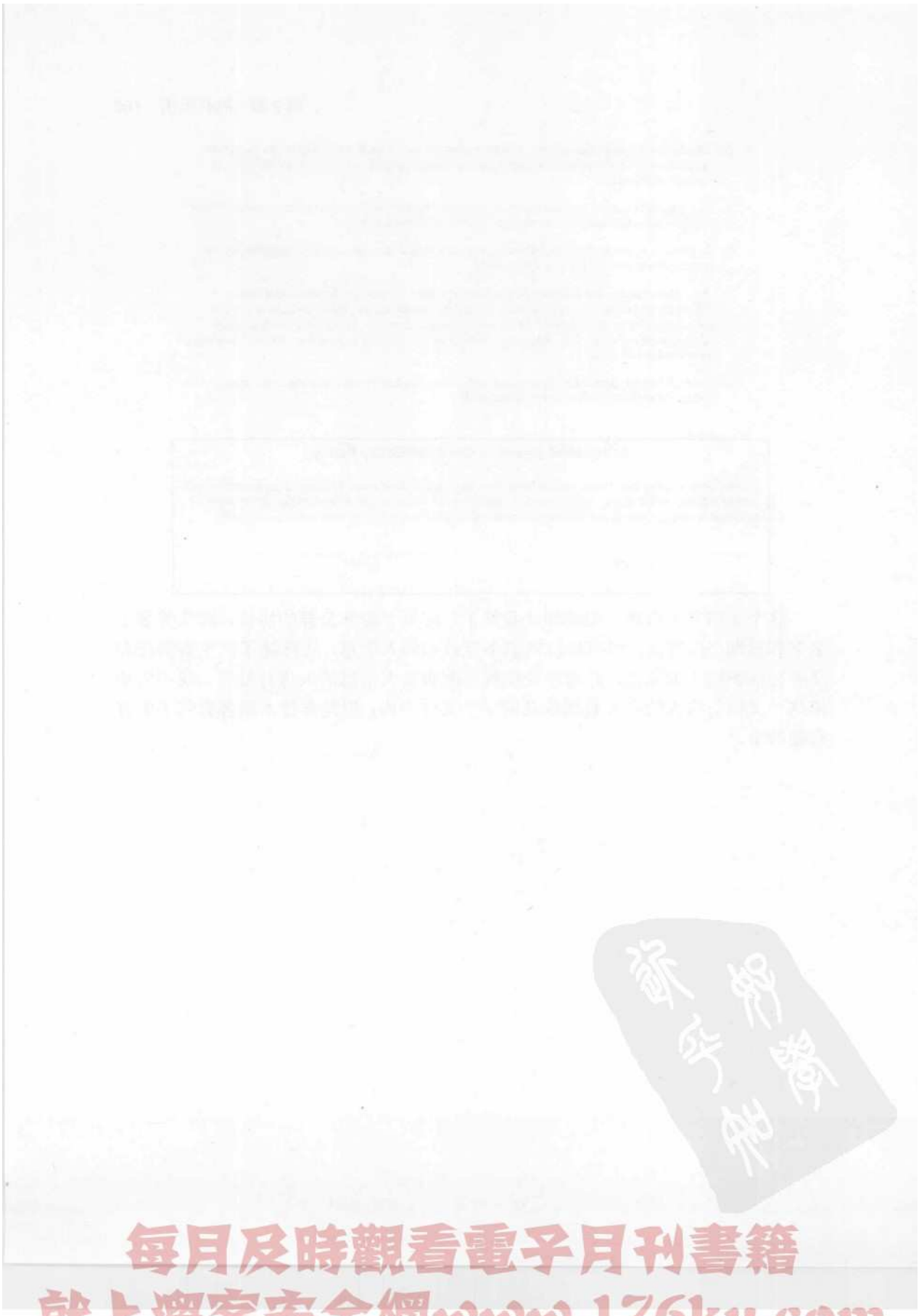
6. This agreement supersedes all previous agreements, written or oral, relating to the above subject matter and shall not be changed orally.

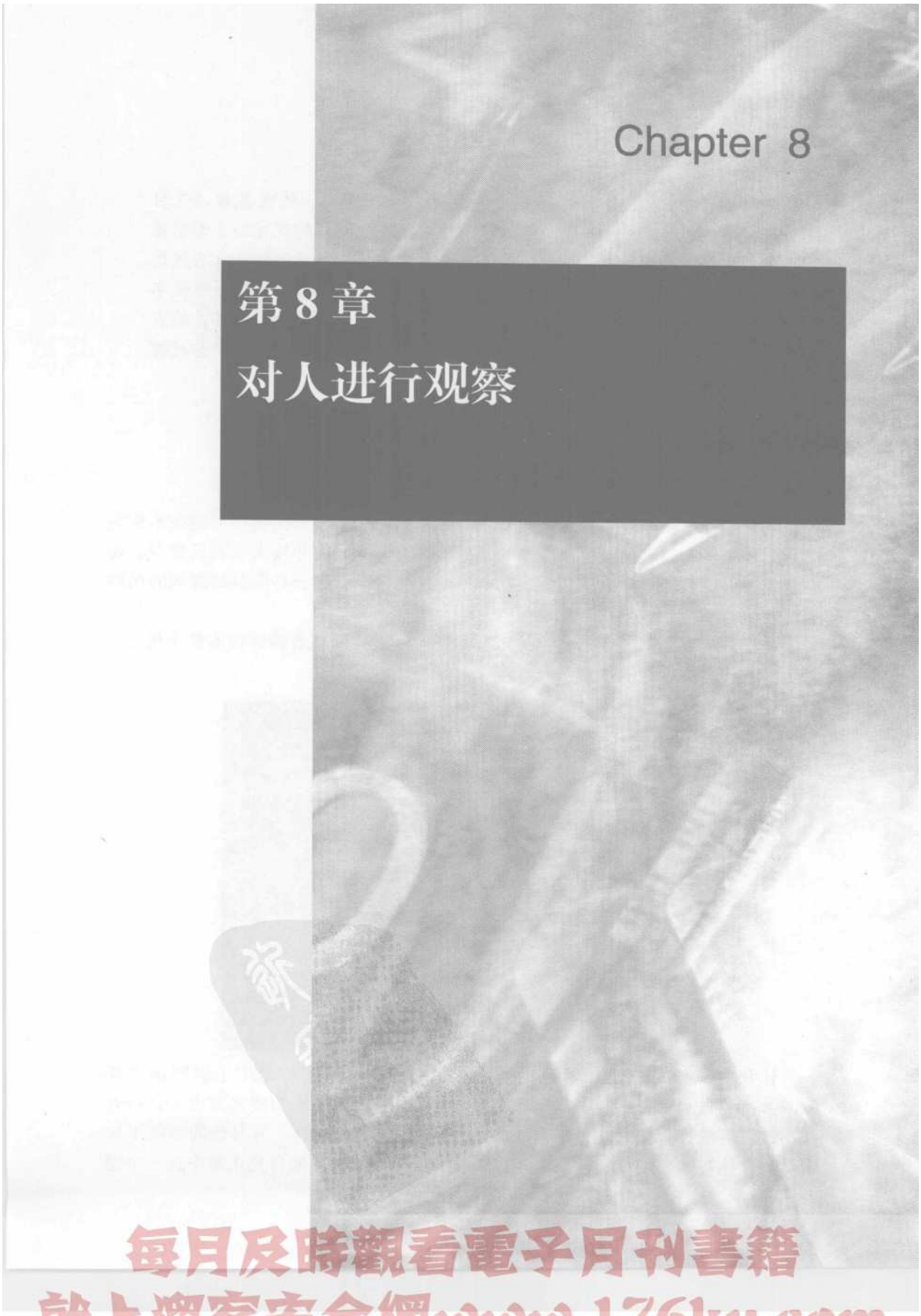
Acknowledgment of Confidentiality Policy

I herby acknowledge that I have been informed of State and Federal Laws relating to the protection of patient medical information. I understand the penalties for unauthorized release of this information. I have had an opportunity to ask and receive answers to questions regarding this confidence policy.

Signature _____ Date _____

这个文档并不有趣，但是却让我笑了。这是一份非公开的协议，医生签署了名字和日期，内容是：没有经过同意不能散布病人信息，还陈述了医生有责任和义务去保护病人的秘密，并对没经授权而散布病人信息的人进行处罚。我不敢相信这个文档与病人的私人数据放在同一个文件夹内。但是非技术黑客看到了所有有趣的事。





Chapter 8

第8章 对人进行观察

Scott Pinzon 是我的朋友,也是本书的技术编辑，他很喜欢《来自 Ipanema 的女孩》这首歌。但是歌曲里观察这个女孩的花花公子却明显是个很业余的观察者。如果他看了本文，可能已知道她住的是什么旅馆（通过观察旅馆的钥匙卡）、可能的收入（通过观察她的拖鞋是在沃尔玛买的还是 D&G 的），以及她的房间号码（通过背后偷窥服务员的方法从而由她的账单来得到她的房间号码）。熟练的观察者通过一瞥能得到很多的东西。本章展示一些非技术黑客眼力的例子。

怎样去观察

对人进行观察是一种真正的技巧，有关这方面的内容很多,我不可能在本章完全介绍。观察人的确是一个很重要的话题，因为一个好的非技术黑客只要专心观察就能很好地判断一个人的情况。在本章，我们将会看到一些简单却深刻的观察人的例子。

让我们从下面图片中的那位绅士开始吧——最前面戴着棒球帽的那个男士。能告诉我一些关于他的事情吗？

让我们从长靴开始。尽管我无法从一次高技术秘密行动中了解阿迪达斯 GSG9，但可以肯定这是战斗靴。那牛仔裤很漂亮，除了他的皮夹露出牛仔裤外（不过我可没打算把它拿过来以获得这个家伙更多的信息），并且他的黑色 T 恤告诉我，他是一个硬汉（或是十分想要成为一个硬汉）。他目光正集中在一个空

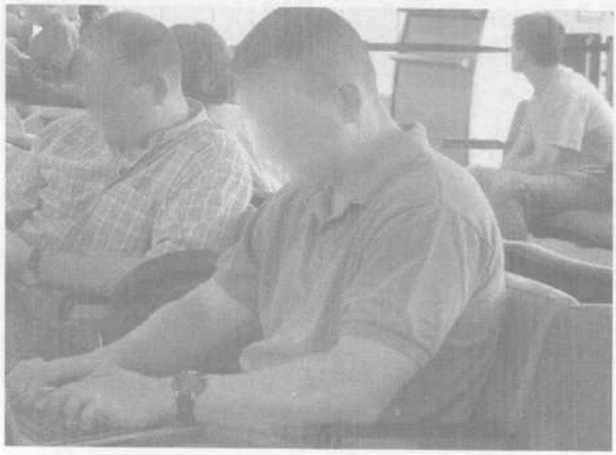
姐那儿，这正好印证了他的硬汉形象，同时也知道了他的性取向。尽管不能过早地将他的发型描述为部队里士兵的那种发型，但是可以肯定他留的是短发。他戴的眼镜是 Oakleys 牌的，并且我听到大家把它叫作射手，因为这种眼镜经常跟枪以及射击的人联系在一起。他戴的是棒球帽，后面的标识很难辨认，但下面有一张更近的图片。

帽子上的标识是 BenelliUSA.com。下面是 Benelli 网站页面的一张截图。

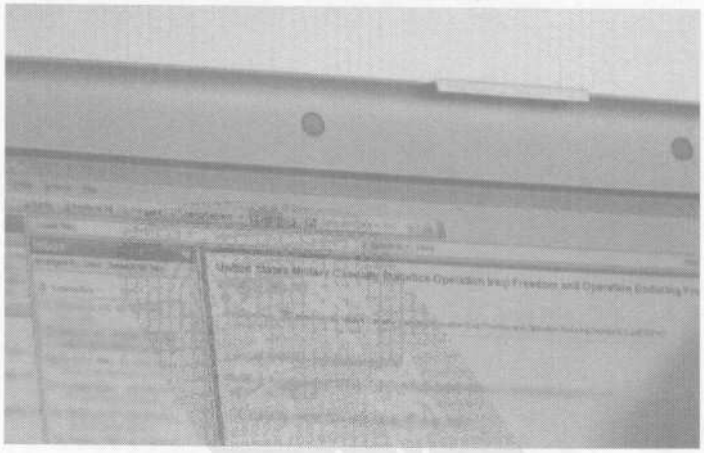
谈论 Benelli（伯奈利，著名枪械品牌）的枪就像谈论 NASA（美国国家航空

航天局）的火箭一样。Benelli 制造的强大穿甲霰弹枪好像内置了导弹运载器和火焰喷射器一样。当然，他们没有制造导弹运载器和火焰喷射器，但是为猎人、水兵和警员制造了强大的武器。猜猜这个家伙是 3 个中的哪个？确定好了吗？我可以说这个家伙不是执法人员，就是军队的——很可能是特种部队的成员。让我们假设在他搭乘飞机时，站在他前面的是一个坐轮椅的老妇人而不是空姐。这样会不会改变你对这个家伙的印象呢？反正那将会改变我对他的印象。

让我们看另外一个例子。认真看下一张图片。



这个相当简单，快速浏览一下。发型：平头；胳膊：强健和棕色的（肘以下）；其他：一枚婚戒和一块 Iron Man 手表。给人的第一印象很明了——已婚，并是军人。



一次快速的背后偷窥证实了这些。他正看的电子邮件主题是“美军伤亡统计”，并且收件箱有来自陆军中校（LTC）和陆军少校（MAJ）的电子邮件。我

真的不关心这家伙是从事什么的，因为我不是一个坏家伙。然而，如果我是一个坏家伙，将在非常短的时间内得到许多关于他的信息。

让我们再看一个例子，看下一张图片。

我背对着他站着，使用我的照相机的旋转镜头往后面拍摄。在拍摄过程中，被我的衬衫挡住了一点，照片的边缘有点模糊。但是看看我的目标，我们看到了休闲裤、黑色的袜子等，他的衬衣像是很随意的商人打扮，尽管是那种略带粉橘色的奇怪的样式。他戴着精美的手表和一枚大戒指。他看的是有关财政和新闻之类的杂志。

到现在为止，他似乎是一个管理人员，但接下来的经历告诉了我更多的东西。我向他靠近，站在他旁边并给他的包照了一张照片，下面就是那张照片。

那个家伙好像并没有注意到我站在他右边，并给他的包照了一张照片。包上有美国政府机关标识，这标识最近在国际新闻现场出现过。因为政府机构有非常

特殊的使命，并且最近公众对其也很感兴趣，我知道总有人将对那家伙从哪里来到哪里去非常感兴趣。我回到了原来的位置，进行了一连串拍摄。

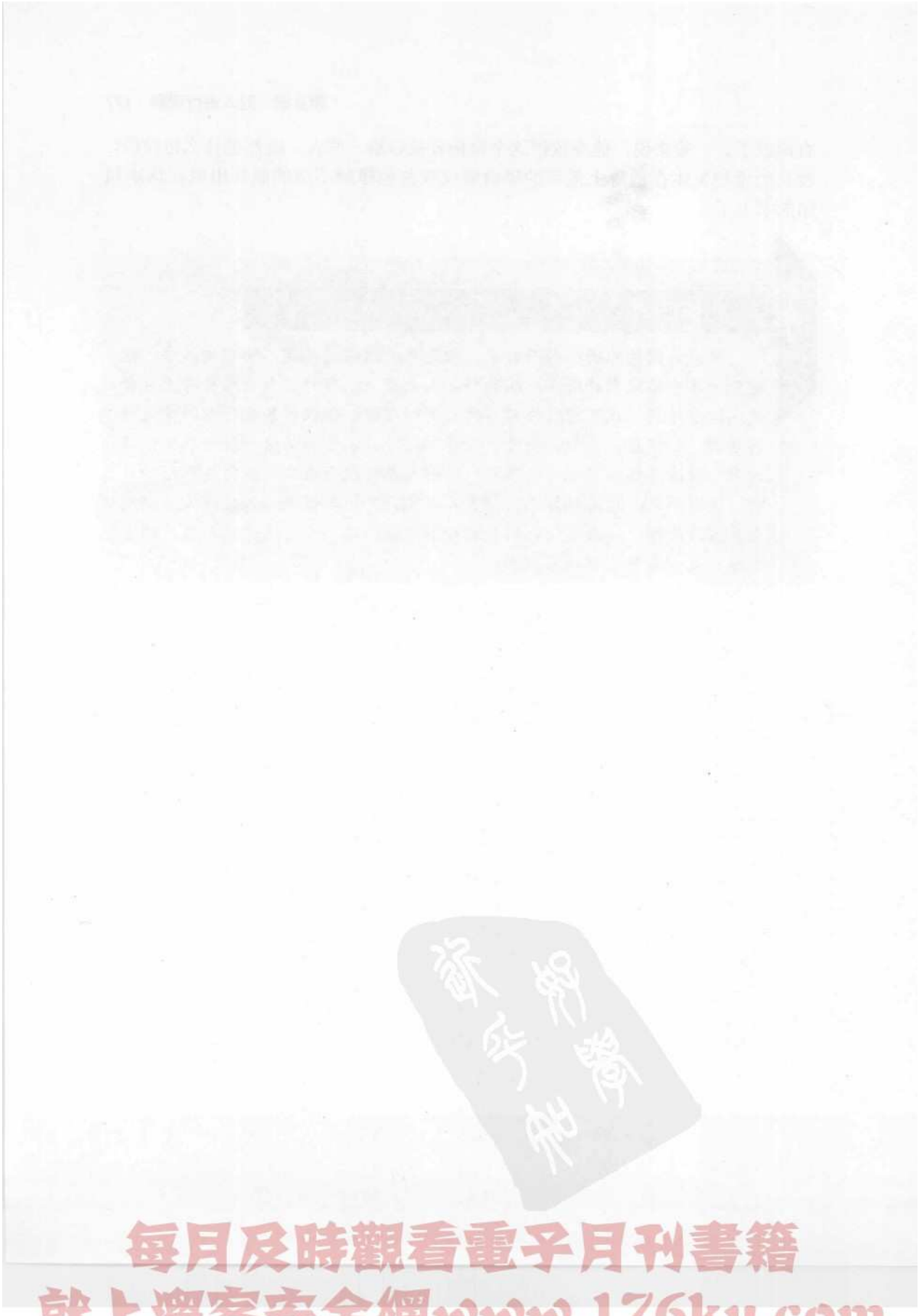
当时我并不知道，但是当拍摄时他正好看到我的镜头并给我这一表情。我真的希望我能够把他脸上的表情显示给你，但不想泄露别人的秘密。相信我，他给了我这种感觉——你为什么要拍我，你这个该死的恐怖份子。如果我当时知道拍照时他正看着镜头，我想可能就没有机会拍到如下一张的照片，从而获得他名字和经常乘坐的航班号。

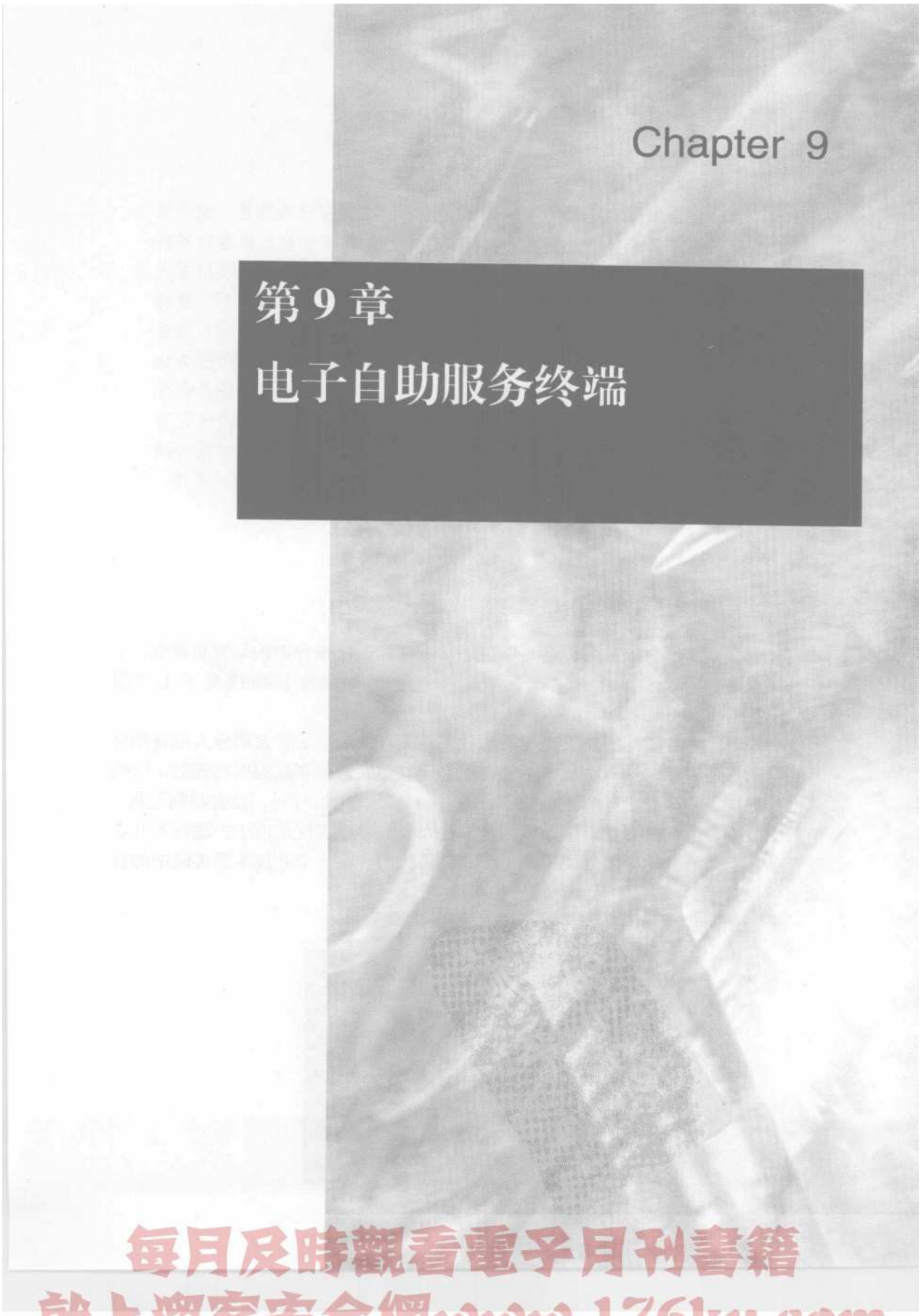
这个例子最令我吃惊的是那家伙已经看到我在偷拍他。他极有可能看到我拍了一些照片，并且甚至观察到（我想是的）我在他周围移动以便拍到有关他及其物品的一些照片。我知道他是为政府机关工作的，但是不确定他为什么没有对我采取行动。我没有任何恶意目的，但是他并不知道这点。就他所知道的，我可能是一些在机场偷拍他的跟踪狂，或者更糟，我可能是外国政府派来跟踪他的人。我没有告诉他我是谁，但是这家伙的选择和大部分人一样——什么也没做。这就

有问题了。一般来说，他应该把这个偷拍者报告给一些人。既然他什么也没做，我只能希望发生在他身上最坏的事情就仅仅是他模糊不清的照片出现在这本粗陋的书上了。

行事低调

你或许因为你的公司而自豪，但是有时炫耀团队是不明智的做法。这些例子集中体现在政府和军队的公务人员身上。有时在企业雇员身上也会发生这些情况。我不想对任何具体人进行指控，仅仅对某些行业的情况进行举例：如银行、金融、制造、投资、医疗、零售和其他一些行业。依据时事、政治气候和其他一些因素，任何人都可能变成公众探讨或讨厌的目标。这些年来，政府机关已经一直要求雇员外出要低调，但政府人员仍然在暴露政府标记。我建议他们最好行事低调。花一些时间考虑形象，经常想想，至少要留心非技术黑客。





Chapter 9

第9章 电子自助服务终端

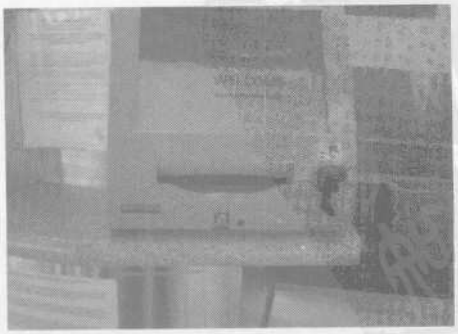
这些自助服务的电子终端到处都有。它们在那里自鸣得意，嘲弄着非技术黑客，求着非技术黑客去破坏它们。但是想想非技术黑客行事的方式，他们大部分时间只是看着它们。正如所知道的，黑客是不用常人的方式行事的。当黑客看到了一台自助服务设备开着时，暴露的信息将超过想象。当自助服务设备暴露更多信息的时候，会发生什么呢？当自助服务设备存有航空乘客的信息时又将会发生什么呢？当自助服务设备存有机密的病人的信息时又会发生什么呢？当自助服务设备存有现金时又会发生什么呢？非技术黑客处理这些设备会有什么不同吗？可能没有。毕竟非技术黑客的方法很有效。但是实际上如果非技术黑客决定去接触这些东西，那将变得很有趣。他们或许真的会干一些坏事情，例如按 Shift 键以侵入这些设备。

了解自助服务设备攻击

一台交互式的自助服务设备是通过电子方法提供数据存取的计算机终端。交互式自助服务设备有时类似电话亭，有时也能够坐在长椅或凳子上使用（http://en.wikipedia.org/wiki/Internet_kiosk）。

如今，自助服务设备到处都有,没人比黑客更了解它。尽管大部分人没有把交互式自助服务设备当成一种安全威胁，但是记住，它们是和数据库相连的，这些数据库存储了许多让人感兴趣的数据：姓名、地址、电话号码、社会福利号码、信用卡数据、银行信息甚至医学数据。虽然大多数黑客仅仅是由于兴趣而弄开这些设备，但是恶意的黑客可能不满足于此。让我们看看一个非技术黑客眼中的自助服务设备吧。

下一张图片显示的是一台典型的机场用的自助设备。

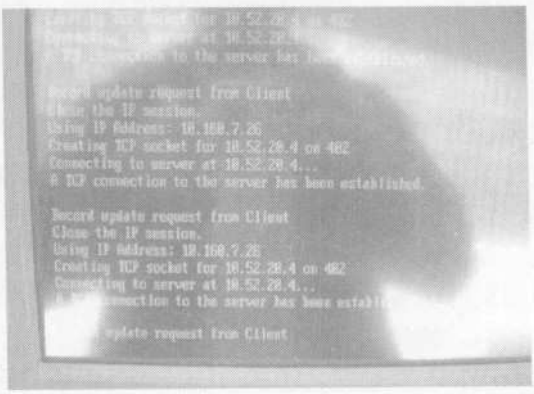


当看到这样一台机器时，我问了自己一些问题，想知道它运行的是什么操作系统；当知道这机器是联网时，想知道使用的协议类型；如果它是在 TCP/IP 协议上运行的，还想知道使用的地址和端口。但是，仅凭空想，要得到机器的网络地址恐怕是不可能的，用传统的方法去找到这些问题的答案需要相当大的工作量，因此得采用其他的方法。

首先，必须找一个地方，能进行入侵自助服务设备的网络。然后（假设我知道机器使用的网络协议），需要把机器连接到网络且开始对网络流量进行嗅探，以便发现某些信息。如果网络中没有数据包产生，我必须开始扫描网络尽量让机器作出响应。一旦自助服务设备作出反应，我将进行分析，猜测它的操作系统。一旦确定所有这些信息，就能形成攻击计划。我认为这是一个无聊的办法，我的意思是这是一种常规的，没有任何新意的做法。如果我想得到更多有趣的东西，将攻击自助服务设备的输入端口。屏幕上的键盘可以忽略（它当然不允许我进去破坏），我将把精力放在攻击信用卡上。我可能会跟踪一张、两张或三张信用卡，并通过读卡机复制，使自助服务设备为我所用。只要我觉得高兴，将使用伪造的护照装载所有的恶意数据并通过读卡器复制卡去破坏它。为了覆盖整个基数，我可以制造一大批伪造卡和护照，并让它们都通过（同时跳过大量的 TSA 代理机构），当然最后有一些东西将会毁坏。我将会因为正式拥有的东西而狂笑，因为一台机场自助服务设备几乎就是我的囊中之物了。

或许在我生活的每天，都可以利用各种非技术手段，睁大我的眼睛，即使在从事完全合法的业务时也是如此。或许之后我将看到像这样的一些东西。

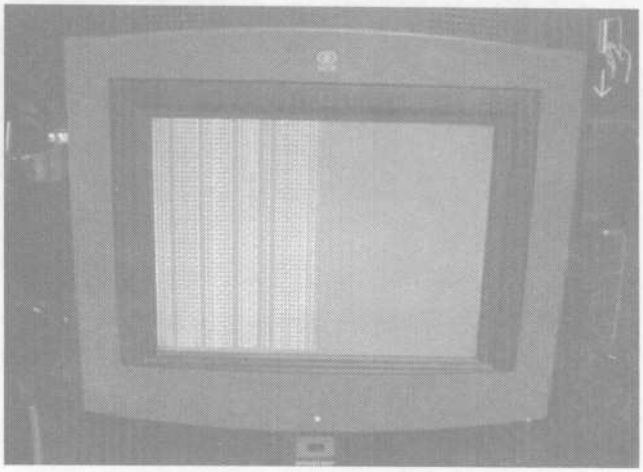
这是我偶然拍下的一张照片。



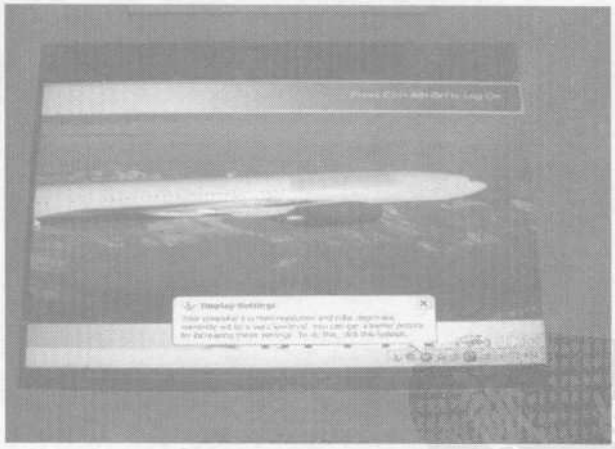
然后，我知道了自助服务设备运行了 Windows 内核的系统,因为只有 DOS 才使用那样丑陋的字体，DOS 在网络方面做得并不是很好，所以这不是一个命令外壳，而只是一种单用户模式。我还知道它是使用 TCP/IP 网络协议的，自助服务设备用的 IP 地址是：10.160.7.26，这是一个私人网络，因为它使用了预留的“10.”的地址，该自助服务设备和一个地址为 10.52.20.4 的服务器相连，并试着连上 402 端口，IANA（国际因特网地址分配委员会）规定这个端口是由一种被称为 Altiris 的产品所使用的 Genie 协议使用的。我朋友 Chris Eagle 做的下一步研究非常好——他建议在 Google 上搜索“Creating TCP socket for”“on 402”，以证实自助服务设备在运行 Windows 系统、Altiris 软件以及错误的信息是来自 DOS BootWorks。我知道所有的这一切都没有接触机器或网络，也没有触犯任何非法的东西。这就是非技术黑客的操作方法。

一个非技术黑客已经知道公用网络电话之类的东西（如下图所示）的运作方式。

一个非技术黑客只要稍留意就可知道网络电话当前正在运行的是隐藏在 DOS 环境下的 CHKDISK 程序，由于硬盘非常差，而且在劣质的装置上的文档记录也很不安全。非技术黑客会知道所有这些，因为下面的图片证实了那愚蠢的东西将会说出一切。

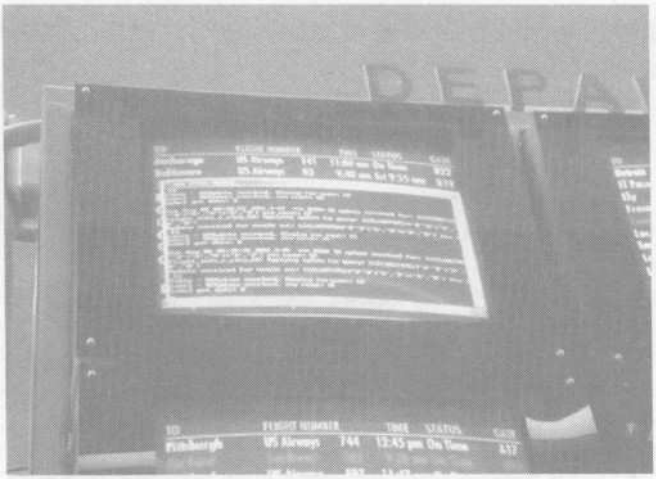


机场信息屏幕很容易就能读懂，尤其是当它们出错的时候。下面的图片显示的就是一个 Windows 任务栏。



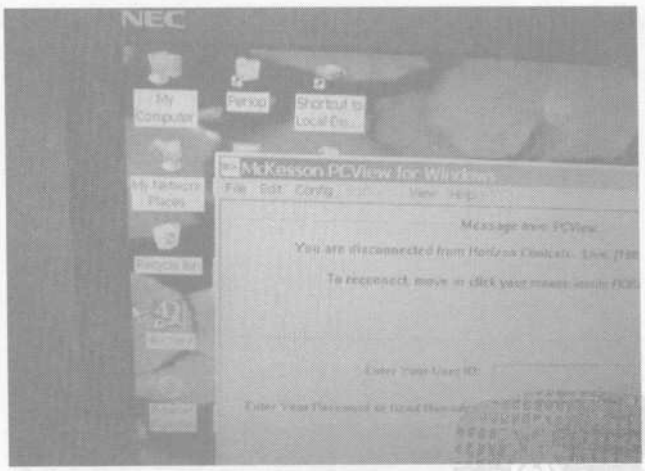
在第 3 章中我们已经讨论了每个图标的意义。我们知道终端在 Windows 上运行，并且机场使用的是 Symantec 公司的反病毒软件（左边的第 5 个图标）。

下图显示航班时刻表也处于非技术黑客的视野内。

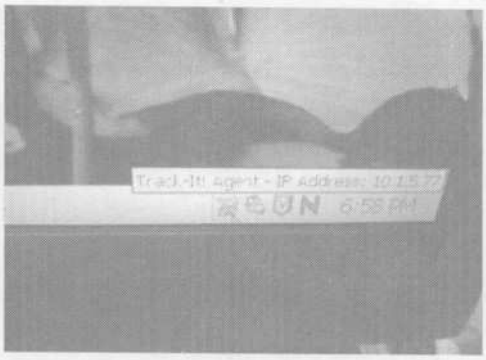


这个界面显示的信息包括存放航班起降信息的数据库、正在使用中的地址及协议，甚至完全自定义的应用程序，然而用 Google 搜索各类诊断信息并不能显示任何东西。

撇开机场的终端，来看一个典型的医院终端。即使非技术黑客们在医院时，也非常好奇。看下一张图片。

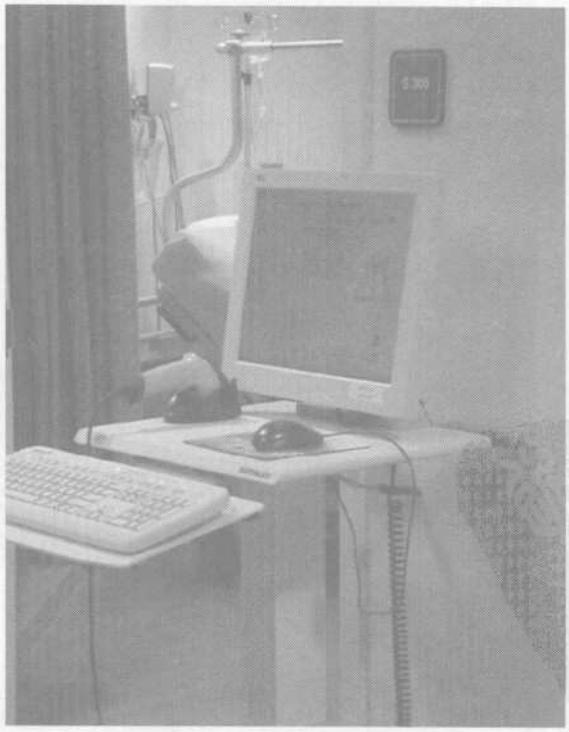


界面显示的是流行的 Windows 操作系统，以及两个有趣的应用程序：McKesson PCView 和 4dClient（有强烈的 NOVELL 公司的味道）。下一幅图是那张图片的另外一角。

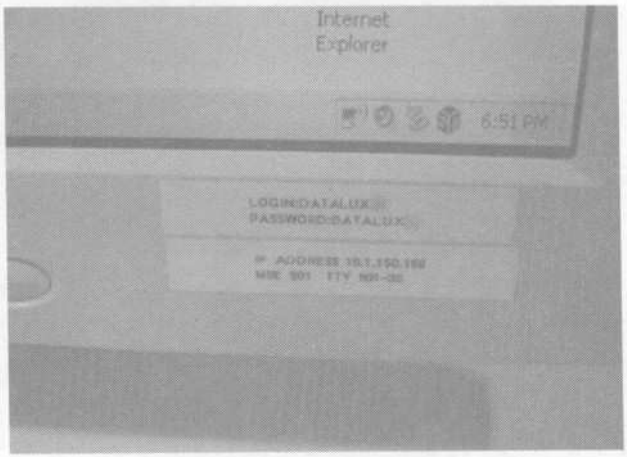


那个大的“N”意味着一个 Novell Netware 客户端程序，之外还有 McAfee 公司的反病毒软件图标，以及 Numara 的 Track-It 帮助中心和资源管理软件的图标。IP 地址也是可见的。我知道这些信息看上去并不充分，但是要记住这都是在没有接触键盘，也没有利用任何高技术攻击的情况下得到的。每个信息都是免费赠送的，而传统攻击者为了得到它则必须消耗大量的时间。

医院的移动护士站也是攻击目标。看下面一幅图片，这是一个可移动、支持无线上网的诱人目标。

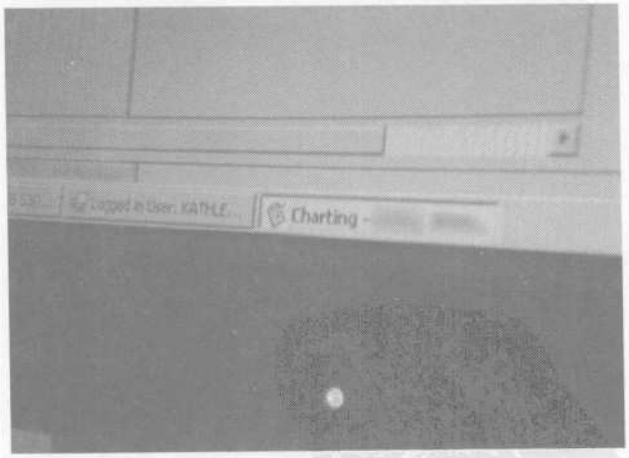


在很远的地方都可以看到机器在运行 Windows 系统，而且活动桌面处在激活状态。靠近一点当然可能得到更多有趣的东西。



因此，一看到这些图标，就知道那机器是无线上网的，并且机器不是静音状态。更有趣的是我能够看到机器在使用 USB 或 PC 卡，时间是下午 6：15。我还能够知道 IP 地址是 10.1.150.166。那是密码吗？对，医院网络的一对用户名和密码写在了标签上面。

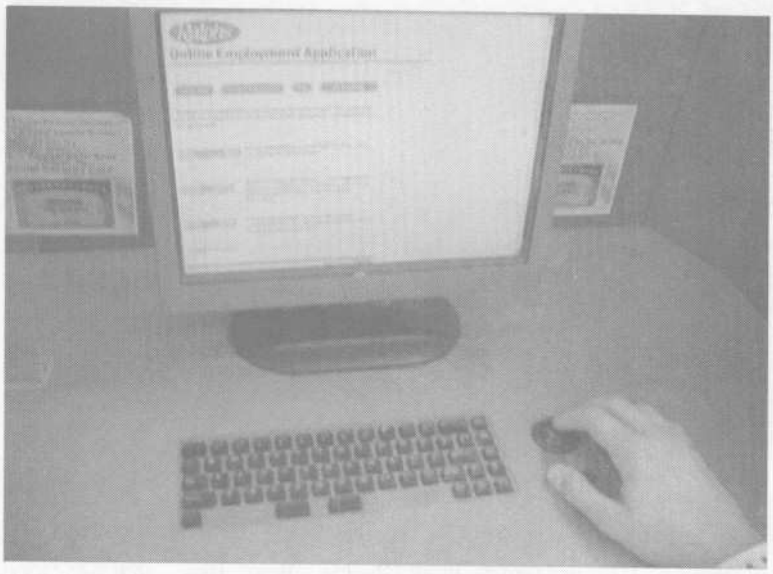
或许说，“但是那不可能是病人的信息”。那就看下一张图片。



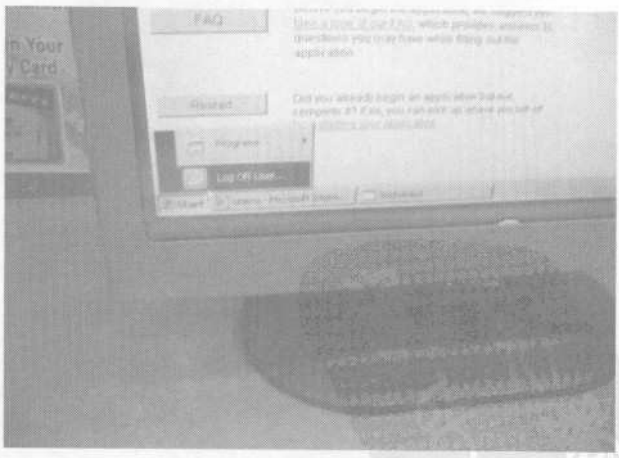
是的，我把图片模糊处理了，但仍可以看到那是一个文字图表，一个病人的图表，上面都是一些敏感的医学信息。

站在附近观察一台交互式自助服务设备特别无聊。终于一个非技术黑客想要去和那个自助服务设备“交流”了。共有 5 个组合键可以攻击大部分自助服务设备，但是我们仅仅介绍一个——一个很少涉及的组合。我的一个好朋友，CP，有

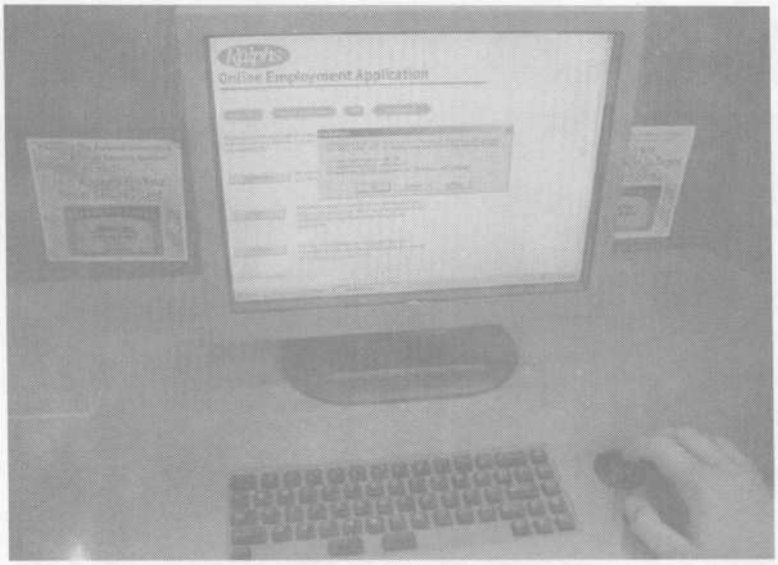
能使机器做疯狂事情的能力，如下张图片所示。CP 拍摄了下面那幅在正常环境下工作的自助服务设备的照片。



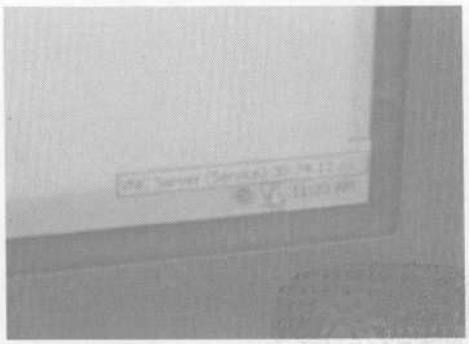
这个特别机器的设计者们特别聪明,他们去掉了恶意攻击者搞破坏时常用的大部分按键。即使如此，Shift 键仍然存在，并且 CP 很好地利用了它。他试了 5 次，感谢 Windows 的粘滞键（sticky keys）功能，自助服务设备伴随着烦人的喳喳声就重启了。下图中的弹出窗口显示了有趣的事情。



下面的粘滞键弹出窗口退出了自助服务设备模式而进入了 Windows 模式。下一张图片显示了 CP 进入“开始”菜单和任务栏的情景。



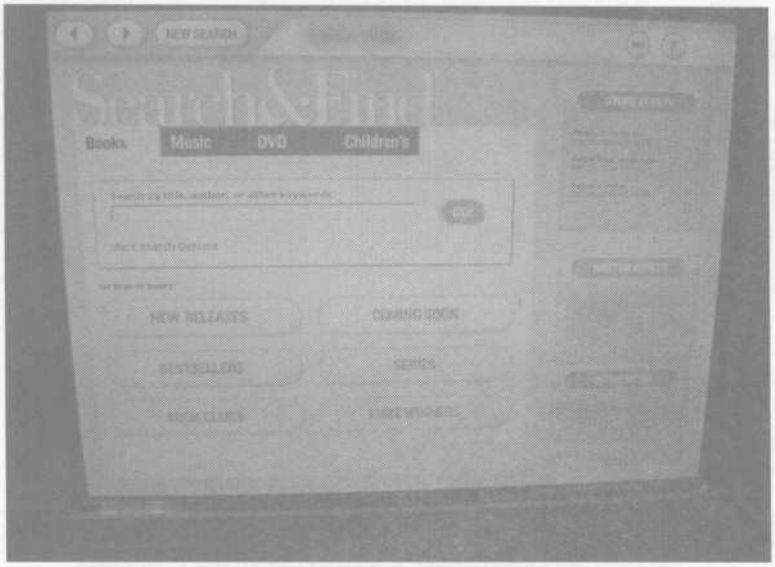
虽然 Windows 会话显示的内容有限，但是任务栏显示了很多内容。我们可以看到设备程序为 Unicru（www.kronos.com），Google 搜索结果显示了这是由 Lowe's, Hollywood Video, Circuit City, Toys R Us, Best Buy, Whole Foods, 以及 Blockbuster Video 一类的软件运行的人力资源应用软件。这非常有趣，因为可以看出粘滞键的“攻击”将被用来攻击其应用程序。下一张图片显示的是任务栏右侧的情景。



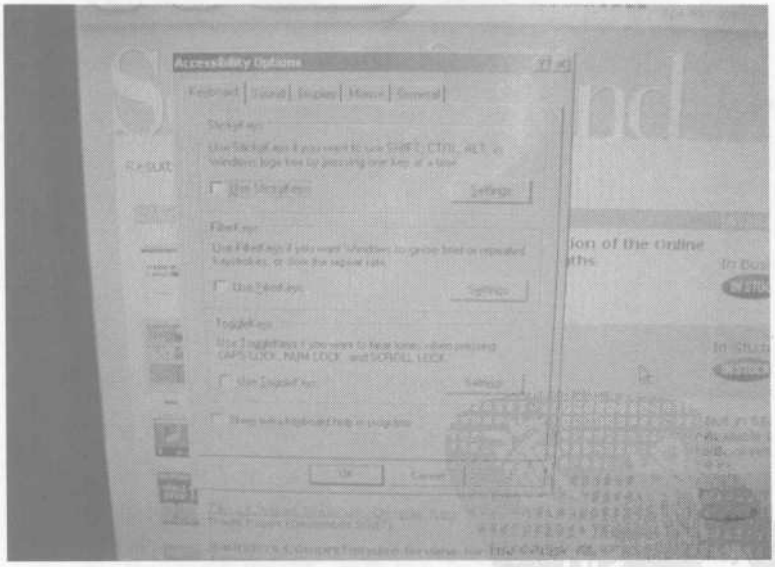
这张图片显示了自助服务设备运行的服务器地址是网络防御信息中心的 VNC 服务器的地址。我不十分确信这意味着什么，但是 CP 的确发现那是美国防御部门控制的主要零售链。这就解释了一些出纳员的军官似的态度。

CP 同时向其他自助服务设备进行攻击。下一图片显示的是一个国家连锁书店的典型顾客自助服务系统。与医院的自助服务设备不同的是，这个是有意放在书店里让顾客去接触的。毫无疑问的是，在漫长的几个小时里，一个技术并不高

明的攻击者就能够在不引起怀疑的情况下引发混乱。



按 Shift 键可以产生粘滞键的配置和其他的一些可选项，如下图所示。

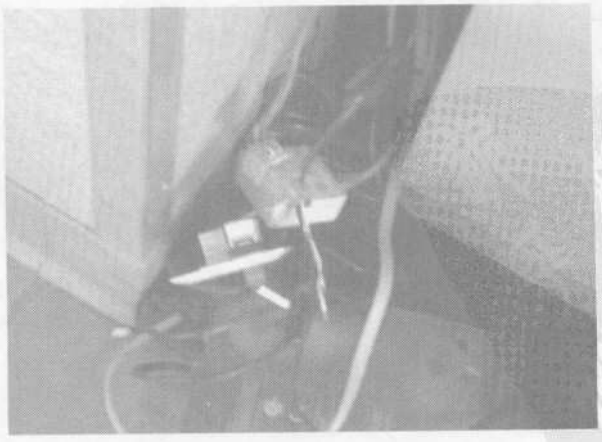


粘滞键的攻击并不会在每个自助服务设备中有效，只是在其中的一些有效，这是另一个普通的非技术黑客能够回避现代安全限制，进行攻击的很好的例子。

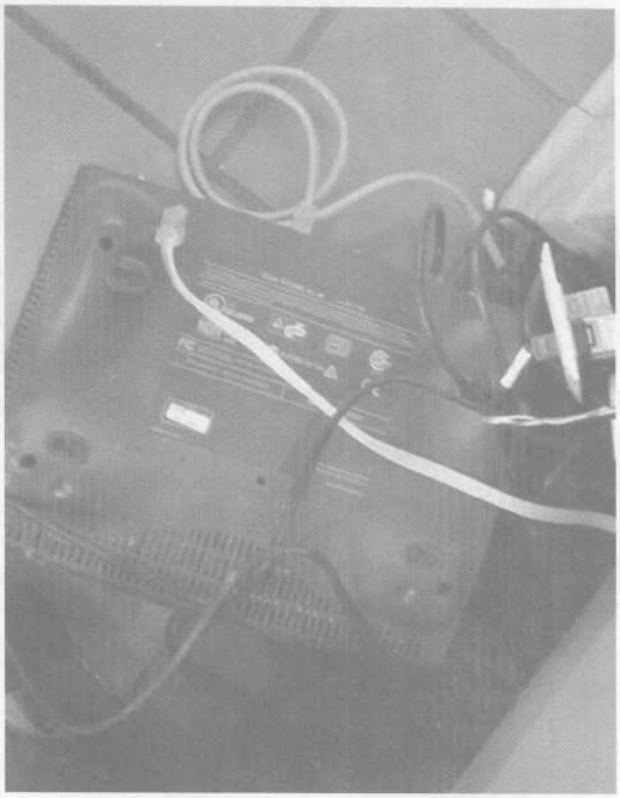
真实的世界：自动取款机（ATM）攻击

电子票务终端、工作智能机、医务记录智能机之类的服务设备是引人好奇的，但毫无疑问的是，自动取款机（Automated Teller Machine, ATM）才是应用最广的自助服务设备。理所当然，它成为所有攻击者（无论是高技术还是非技术的攻击者）的目标，当我看到下图的场景时，我忍不住拍下一张照片。

两位技术员投入地工作，几乎没有注意到我。我拍了几张照片，最后穿着蓝色衬衣的技术员接到一个电话并慢慢地走开了。虽然他仍保持靠近他的岗位，但是我知道他的任务比较多，他已经忘记了周围的世界。我抓住机会靠得更近，站在机器旁边，刚好不在另一边蹲着的计算机操作员的视野内。我低头看去并拍下了下面的照片。

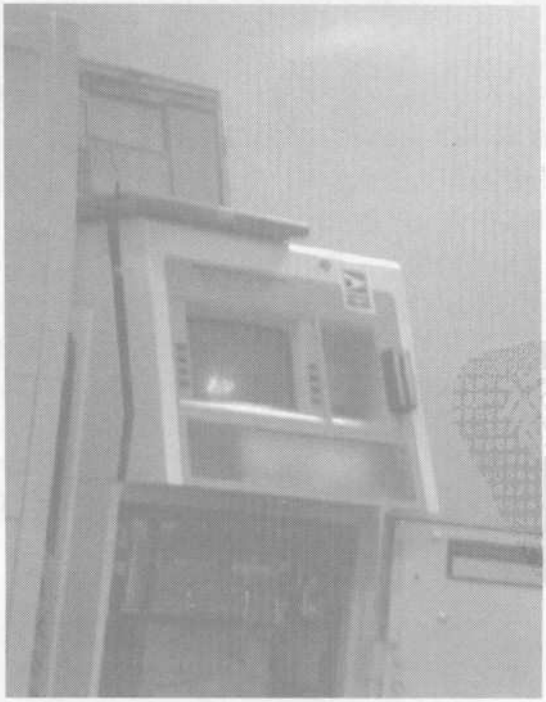


混乱的线非常吸引人的注意。我知道那是标准的网络电缆，认得照片底部的灰色的设备，而且找了一张关于它的清晰的照片。

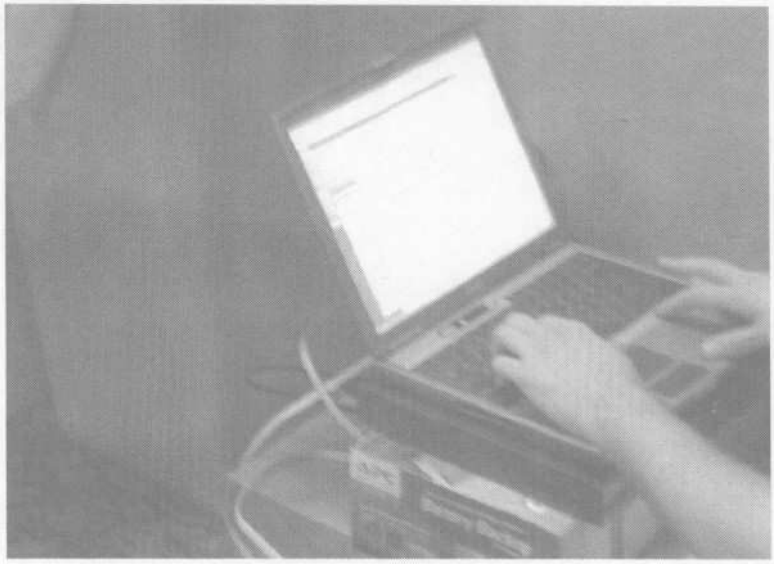


Cisco 1700 系列路由器的确有点旧，但是至少还是可以看出来的。虽然我对 ATM 机没有做过很多研究，但是一直认为它是个古怪的机器，它拥有神秘的硬件和秘密的协议。那根网线提示了我，使用的是普通的协议（类似于 TCP/IP），并且 Cisco 路由器使我更加确信。从 ATM 的后面看，我看到机器后面的网线，并想知道它是否一直都是从机器里面引出来的。这也让我更想知道我是否能过会过来，并连上我的集线器或路由器，然后随便使用机器。当身着蓝衬衣的技术员接完电话回到岗位时，我已经离开那台机器。我知道自己决不会回去尝试关于网络电缆的想法。我知道那样做将会有什么后果，但却没办法抑制住好奇心，穿过礼堂，盯着那个技术员。穿蓝衬衣的技术员打开前面的柜子时手机又响了。当他走开后，我拍了一张 ATM 机内部的照片。

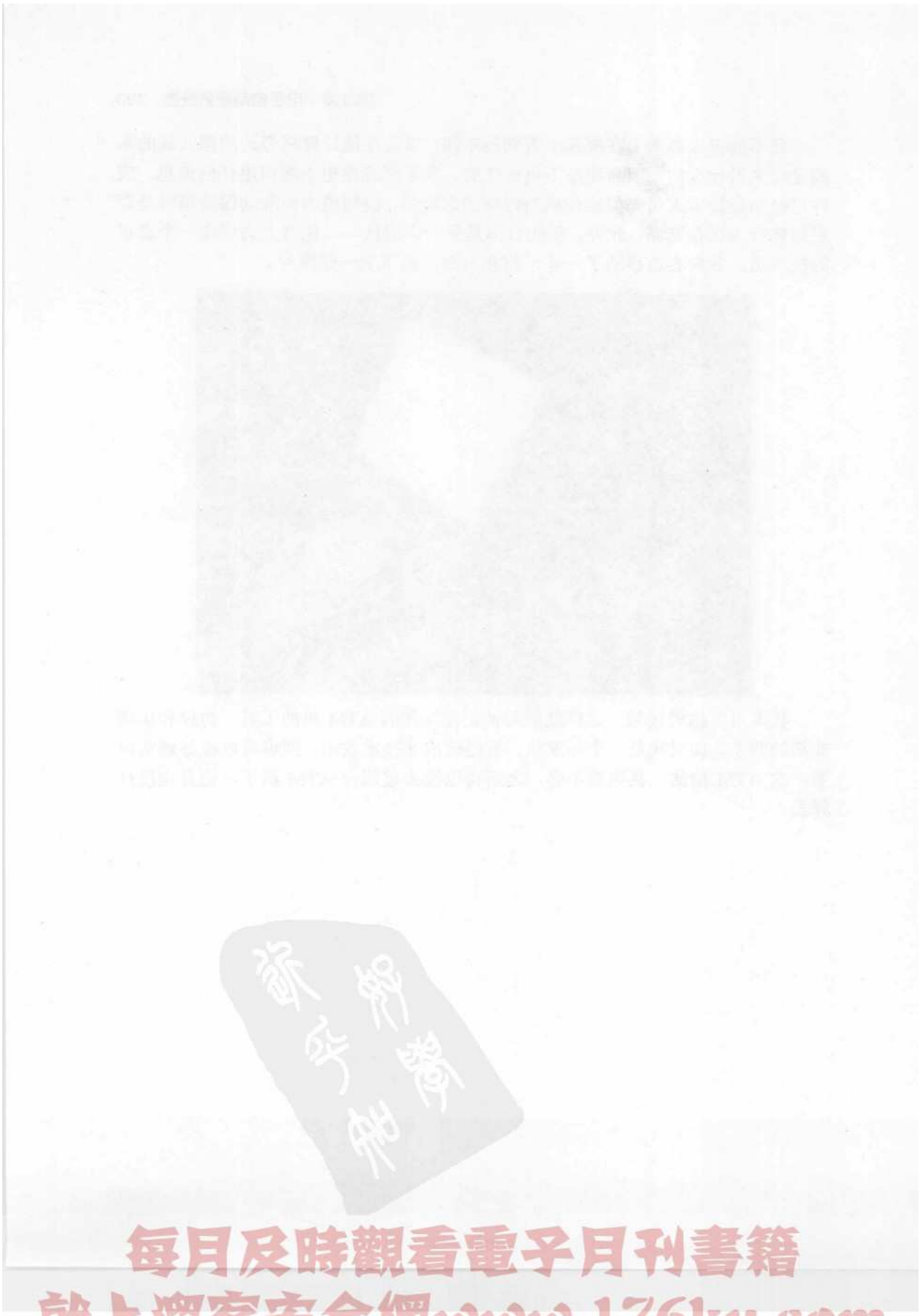
机器里面看上去像个标准的个人计算机桌面。我知道通过 Google 搜索 ATM 机的名字可以获取更多信息，挖掘出它的工作手册（这很有效），这是一个更有趣的事情。我是这里的来访者（我当时是要去做一个关于非技术入侵的讲座），尽管人不是很多，并且明显没有带来访者的徽章，但是偷拍到了一些关于 ATM 技术人员的照片，Google 搜索也不过如此。我拍下了蓝衬衣技术人员的笔记本计算机，它被放在了机器顶部。



我不能说太多关于在屏幕上看到的东西，以及在他计算机旁边的像天线的东西是用来做什么的，因为那是不负责任的。我不能确定也不能拒绝任何信息，或许已经知道技术人员如何操作机器内部的保险箱，也知道当他乱动保险箱时是否对偷窥行为保存警惕。此外，我的目标是另一个家伙——他看上去更像一个真正的技术员。我向右边移动了一些，站在后面，拍下了一张照片。



我本可以拍成视频，这样就能对他正在操作的 ATM 机的工具、协议和步骤非常的熟悉。如果我是一个坏家伙，通过这次非技术攻击，或许可以很好地实现第一次 ATM 抢劫。我当然不会，之后再也没去过那台 ATM 机了，而且也没打算去。



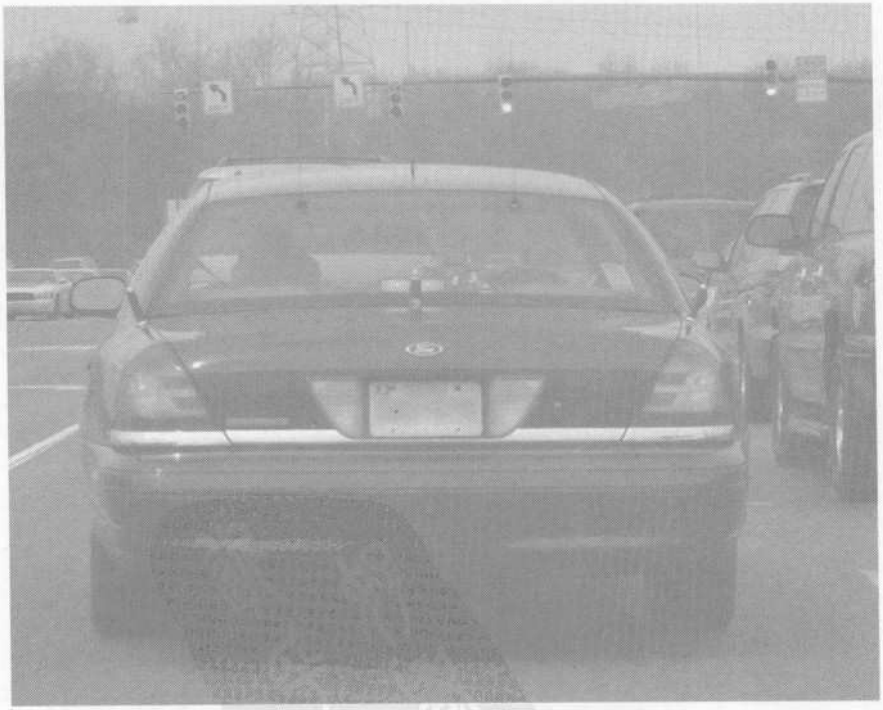
Chapter 10

第 10 章
车辆监视

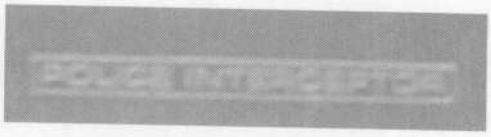
没有哪部间谍电影是没有追车场景的。但是这需要许多的消耗、巧妙的剪辑和大量的预算，所有这些创造了震撼却又虚拟的场景。大部分人都不了解的是：很多针对车辆的间谍活动却发生在车辆静止不动的时候。

车辆监视很容易

无论我是在打算闯入一幢办公楼的路上，或者仅仅在附近闲逛，都会注意周围的车辆。我与爱车族不同，他们喜爱有趣的、古老的或者奇特的车，但是我看到大楼外面的车时都会激动得发抖。非技术黑客就非常擅长这些，在本章我将展示他们寻找信息的方法。看下面的图片，能告诉我关于那个司机的一些信息吗？



好的，从简单的开始。除了窗口露出的竖立的天线，还有一块金属板（见下图），它可以准确地告诉我们这是什么类型的车辆以及司机是做什么工作的。



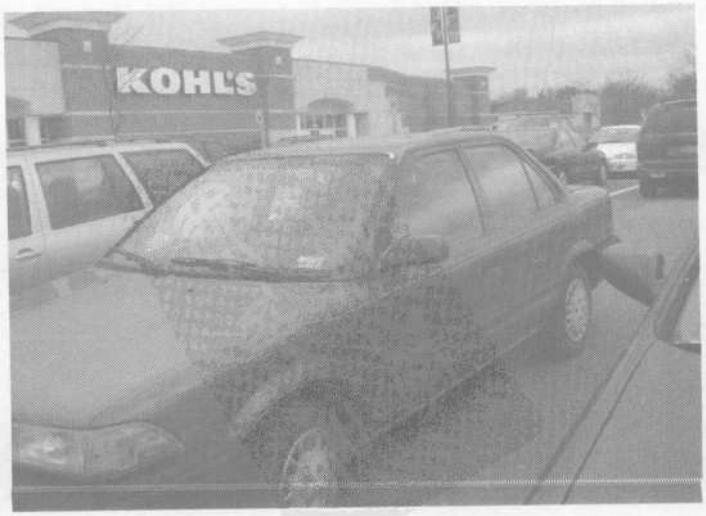
如果你猜那辆车是一辆秘密的或没有标记的警车，那么是对的，你或许已经掌握了车辆监视的诀窍了。进行下一步的猜测，我非常有把握确定司机是一个警官，或者不过是个开着辆警车的家伙而已。

看另一张图片，能根据下面的照片告诉我关于那个司机的一些信息吗？

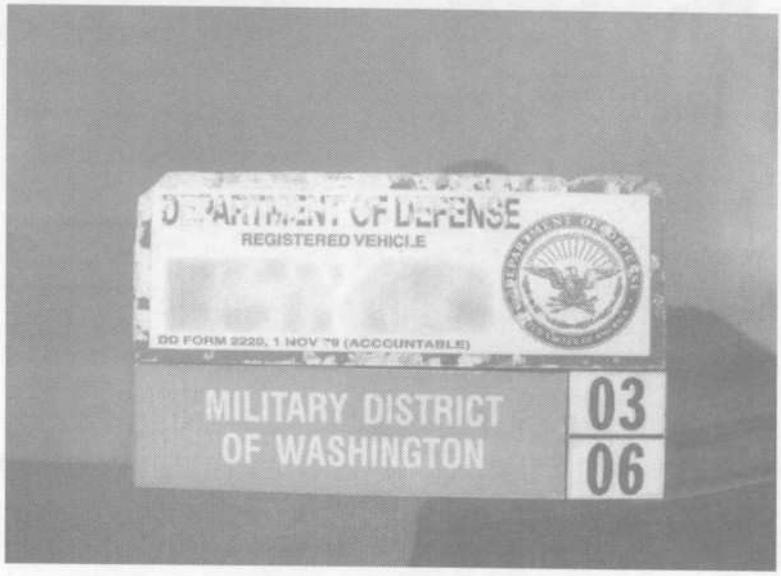
标志是“美国政府”和“仅供官员使用”。如果猜他是政府职员，祝贺猜对了。让我们继续看另一个例子，看下一张图片。显然这辆车司机为了生计而开车，但是一个非技术攻击者会考虑怎么利用这些信息呢？

当我第一眼看到这辆有篷货车，认为是一辆社区服务用车。穿上合适的衬衫，印上正确的标志，我就可以成为这家银行安全和保险服务公司的工作人员，然后可以在这家公司的保险箱、保险库或警报系统上进行工作（这些不是攻击者感兴趣的）。让我们试一下另一个练习，看下一张图片。

大部分普通人仅仅看到一个拥挤的停车场。连一个大妈也立即知道这是 Kohl 百货商场的停车场，并且大家都被这儿每隔一周都挂着的“换季大甩卖”的横幅吸引着。一个像我这样很少看书的人也知道穿过停车场就是 Barnes and Noble 书店。一个非技术黑客则会立即想到“fed”——联邦探员的俗称。他怎么知道这些呢？是从上面的图片知道的吗？如果不知道，看下面的图片，那就是联邦调查局的车。



走近一点，一个非技术黑客将认识到这黑色的车的确是一个政府工作人员的，并且大概知道这位员工的工作地方。所有这些或者更多的信息可以从贴在车上的许可证中获得，如下面给出的图片。



这种标记到处都有，尤其是在有大量部队和政府出现的地方，例如军事基地和国有商业区。下图是几种不同的许可证。

有些许可证也有颜色差异，这些不同的颜色就是标志，它们显示了职员的地位或者等级。有些情况，等级有更加突出的显示，如下图所示。

在这个特别的例子中，用 Google 简单搜索就知道这辆车的主人是美国空军上士。

有些标识很有意思，如下图所示。

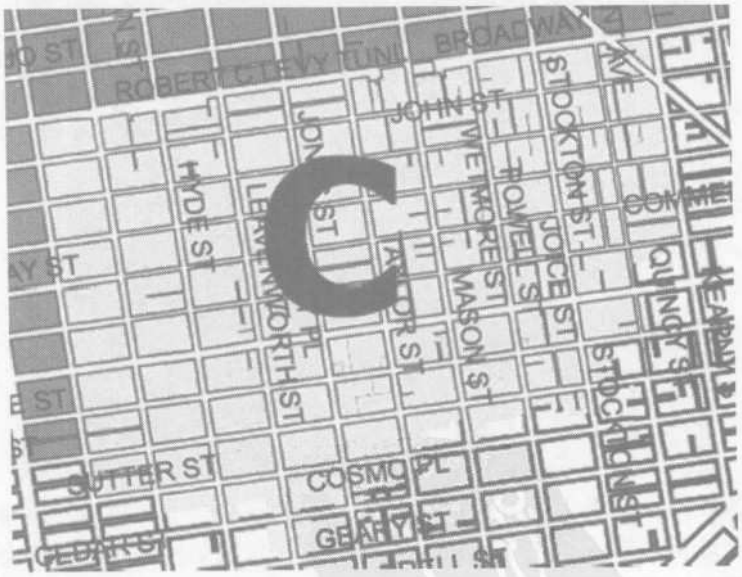
这是为数不多的搞笑标识，是首字母的缩写 IHDIVNAVSURFWARCEN。这是我多年来看到的最长的缩写。政府职员不是非技术黑客唯一的目标，看下图那辆沃尔沃汽车,就可以知道那里不是车主工作的地方就是生活的地方。能告诉我怎么判断吗？

答案不在车的许可证和车辆识别号码上，而是在窗口的标记上，如下图所示。

这样的加油标记看上去好像是没有害处的，但是一个非技术黑客能够很快地推断出那地址可能靠近车主工作或生活的地方。如果车停在工作停车场里，而地址不在这附近，那么它就可能是靠近车主的家。大部分人是不会跑到很远的地方加油的。

有些情况下，通过看他们的车很容易就知道司机的历史记录。从下图判断，能告诉我那司机生活的城市、城市的哪个地方，以及大概在那里生活多久吗？

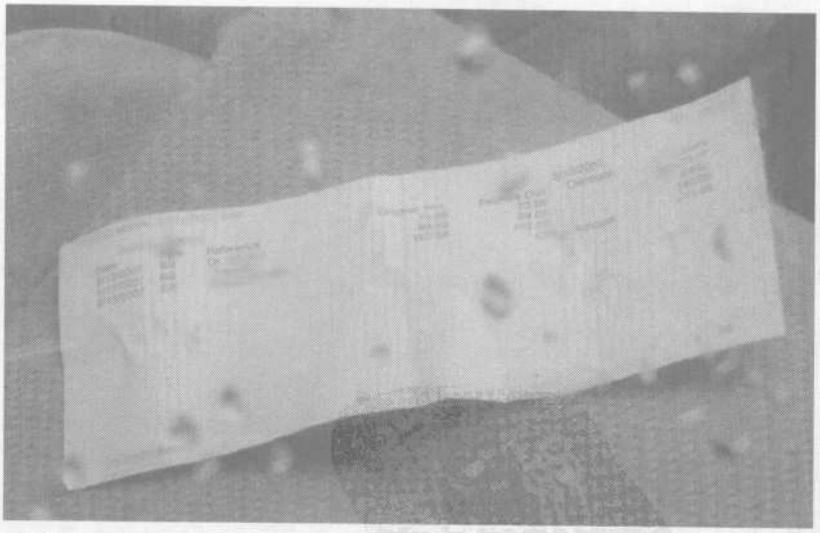
城市是很容易知道的——停车许可证就能够说明这些。鉴于第一张停车许可证终止于 2000 年 7 月，猜测他在旧金山生活多久也是很容易的。想要知道司机生活在旧金山哪个地方就需要发挥点创造力了。但是，Google 是非技术黑客的朋友。快速地搜索旧金山居住停车许可证地图就会生成一张 PDF 格式的地图，下图显示的就是其中的一部分地图。



通过这张有效的许可证，地图清楚地标出了司机生活的大概地方。下图也非常相似，也能推断出相同的信息，但在这个例子中，一个非技术黑客还能够确定那个司机之前生活的地方和什么时候离开的。你可以吗？

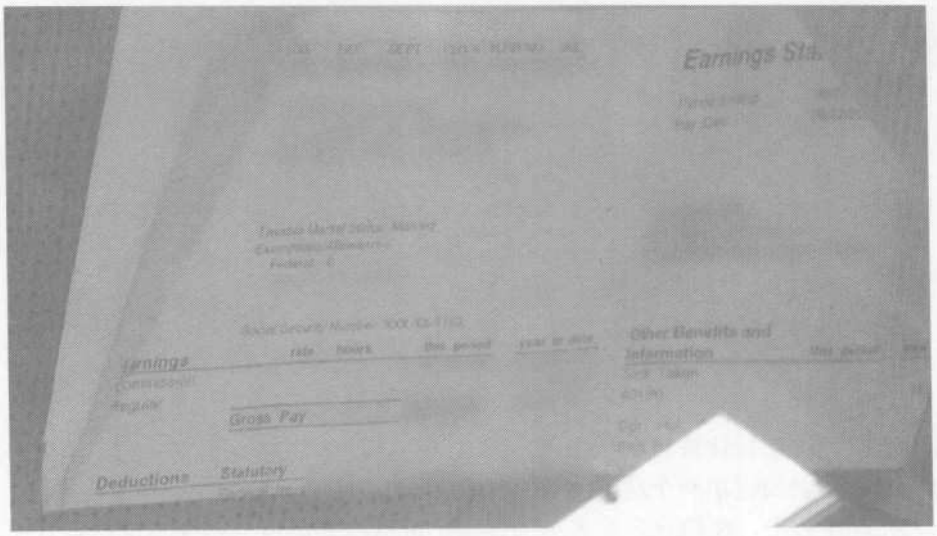
从停车许可证上的数据可以判断，在 2004 年的 2 月至 6 月期间的某一时间，司机从旧金山的居住许可区域 A 搬到了居住许可区域 C。利用 Google 搜索得到的地图，可以知道那两个居住许可区域在旧金山的准确位置。

到现在为止，我们只是看了车的外面。虽然能够通过车外面的标记获取更多的信息，但是最好的一些东西经常是在车的里面，它将告诉我们车经过的任何地方——如下图的收据。尽管我必须把糟糕的相机的镜头焦距从车窗上的雨水移到车内的文档上，但是我认为照片拍得不错。



这张收据列出了医生的姓名、地址、电话号码、病人（估计是司机）的姓名和保险公司、当天的一串详细服务数据，以及这次服务的费用。大部分人对于医疗数据保护得特别好，但是让我惊讶的是，经常能在外面看到这些信息。

对于大多数人而言，财务数据是一项比医疗数据更加重要的数据。我在一个职员停车场拍到了这张照片，文档来源于一个资深的主管。

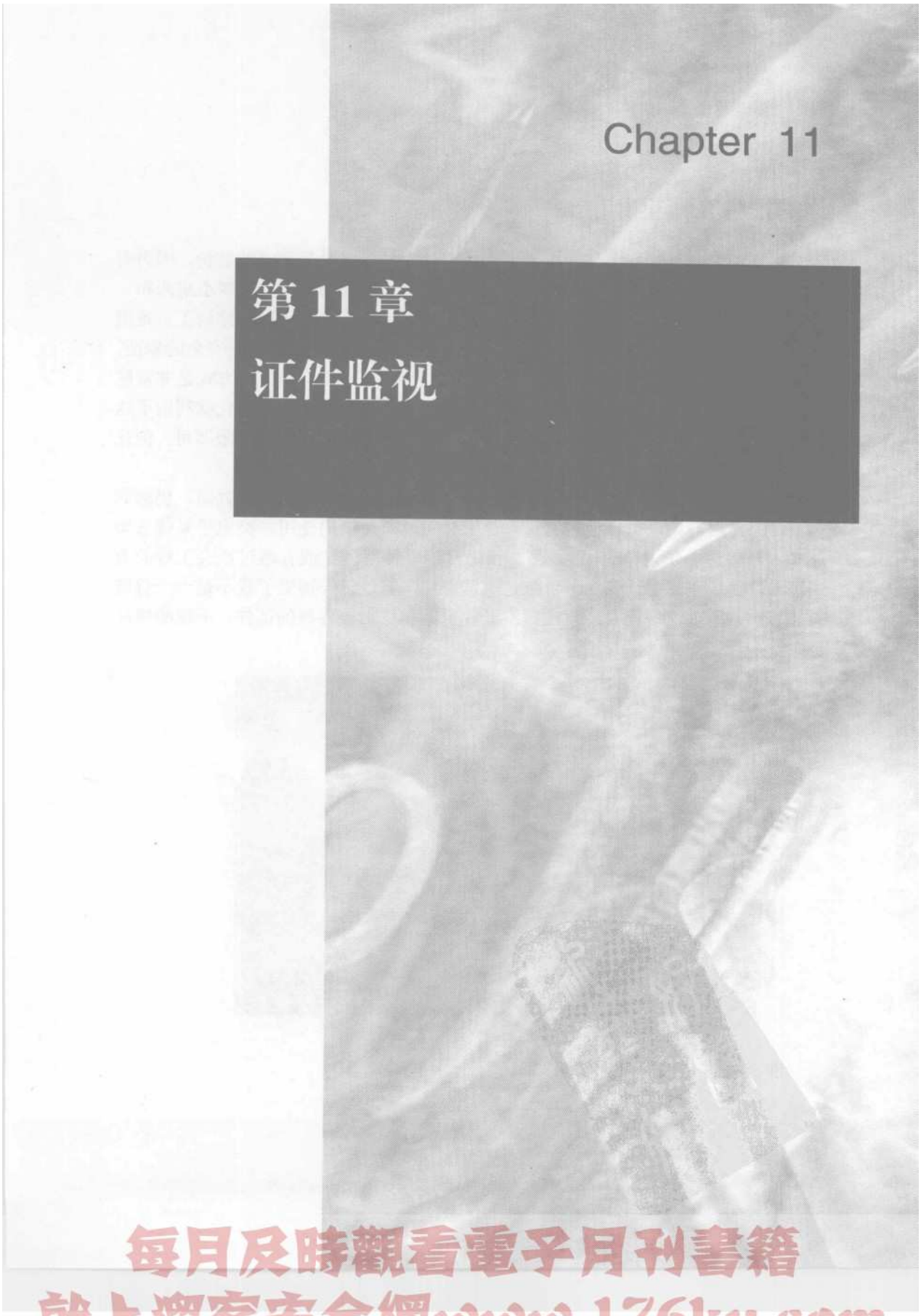


正如所看到的，它显示了职员的名字、效益信息、网络、薪水、税款信息以及更多。在我看来，最有价值的信息就是职员的社会保险号的最后 4 位数字,这些数字关系大部分自动身份验证系统的安全问题。利用这些信息，我能轻易地以这个人名建立信用卡或者窃取完整的身份信息。

当然，在我以这种方式得到这些信息后，会设法进一步获取其他信息。但是下图提醒了我，一些人恰恰对保护他们的隐私不关心。这就是身份窃取不断导致商业犯罪的原因吧！

我不能抵御诱惑了，只能用一句坏的双关语来表达——“见者有份”（It pays to Discover）。这张信用卡的卡号可能被任何买主轻易地用于消费，这些买主不会

遵守严格的信用卡程序，大多数都不会。如果你把医疗记录、银行声明和信用卡放在前面的座位上，非技术黑客极有可能在你准备放起来之前就看到了它们。我已经说过，保护自己最好的方法就是保持警惕，并且试着用非技术黑客的眼光来看生活。在本书结尾会有更好的建议。



Chapter 11

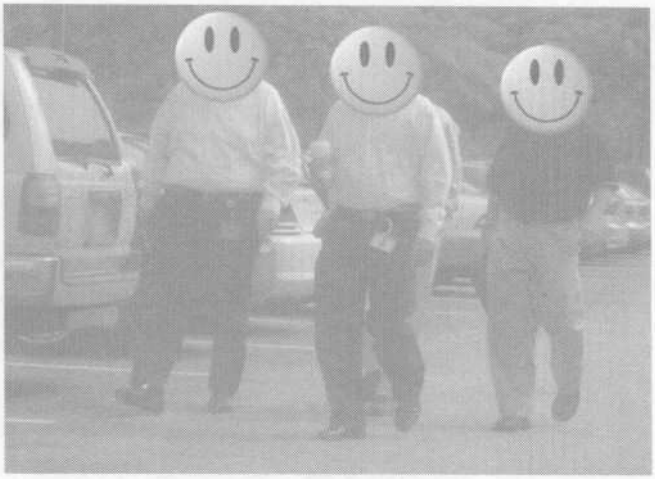
第 11 章
证件监视

你的证件在哪里？

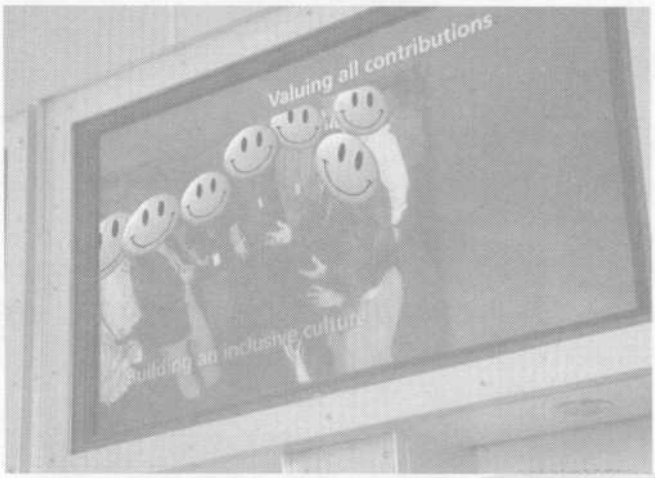
我喜欢像电话维修工一样大大方方地走进大楼，这是最喜欢的装扮，因为有全套装备，而且了解行话。但是没有看上去很正式的证件，只有一些小东西和一件样子很难看的衬衣。但证件能改变外表，外表又让我变成了电话维修工。难道其他都不如一张薄纸管用吗？不是的，有很多东西都管用。但证件是安全的象征。当我向某人出示它时，他们看一下就知道我是谁。基于视觉的认证方式是非常脆弱的，但却是我所测试的大部分建筑物里所采用的认证方式，因此我就利用了这一致命的安全缺陷。复制一个证件对一个攻击者而言只需要偷瞥一眼即可，但让我非常惊讶的是每周都能在外面看到成百上千个证件。

即使我在外面可以经常地发现这些东西，但是当看到一个新证件时，仍感到震惊，因为知道完全可以通过它进入这家公司。即使他们使用各类电子系统去验证（本章将进一步讨论这类系统），我仍然可以使用证件或者通过社会工程的方式进入。我知道证件让我头晕目眩是有些奇怪，但是已经接受了我不是一个普通人的事实，所以这些天我一直在搜索。我带着相机拍摄各种的证件，下图的照片是在一个商场拍摄的。

许多时候，证件会成堆地出现，如下图所示。



当我在一个公司大厅的休息室（当然是基于合法的业务）等候时，被墙上大屏幕里的公司的宣传片吸引了。就在我无意中看到了如下图所示的画面时，马上就拿起相机拍摄，险些从扶手椅子上摔了下来。



画面中显示了一群职员（公司各个部门的人），他们都带着证件。我对入侵这栋大厦不感兴趣，但在大厅里待了 2min 后，得到了足够多的信息去伪造一个证件，并能够用我的方式进入这幢大楼。

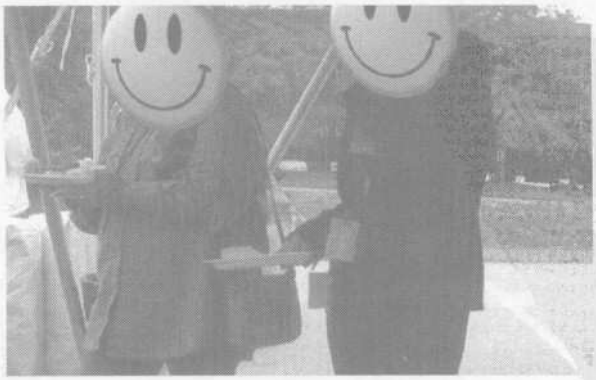
这些年，政府机关一直要求政府雇员离开工作场所时，应当拿掉证件。当强制推行这个政策时，政府雇员从事的工作越秘密，执行这一政策就越积极。在从事秘密工作的政府大楼外很少发现有带着证件的人也就不足为奇了。这里的关键词是“很少”。当我在华盛顿的政府各部门检查时，偶然遇到一个租赁公司在筹办户外野餐活动，活动的目的是为了感谢各类企业承租人员，其中就有一些是政

府人员。当我在大型帐篷周围闲逛时，惊奇地看到了大量的证件。我急忙地拍摄这些人，以至于都忘记吃免费的食物了。

我看到来自不同公司的证件，其中一些比其他的证件更令我吃惊，如下图中的机场证件。

我确信带着像证件一样的纸片是不可能随便进入飞机场的，但是这张图片是引人注意的，这可能会对机场造成损害，考虑到这点，我不得不想起最近发生的关于 TSA（培训服务局）错放了几百件制服的新闻。我既不肯定也不否认当穿着一件（或者不穿）TSA 制服在未经授权的情况下是否能进入一个机场。

当我再次走向公共帐篷附近时，两名排队的女士引起了我的注意（不是因为她们漂亮）。两个人中较高的那个看上去身居要职，她穿着一套时髦的黑色套装，正在通过黑莓手机进行一段的重要的谈话。引起我注意的不是时髦别致的手机，而是她的证件和系在身上的随身用品。我观察了一整圈，也看到了人们身上挂着的各种各样的物品，然而这位女士似乎是最多的。



当我走近时，发现她的证件的确是政府部门的。我照了一些照片（她们都没有注意到），发现引人好奇的证件上有个特别的东西。当她继续用手机聊天时，在不惊动她的情况下，我转到她的另一侧并尽可能走得更近，在离她不到一英尺的距离内，我拍下了下面的照片。

这个特别的证件是发给五角大楼的职员配戴的。后面的便笺提醒她“带一个昨天的副本去 DSS H.Q.”。当然五角大楼的安全是首屈一指的。依个人经验，我知道五角大楼的警戒应当很严，他们不会对安全视如儿戏的。我也知道一张证件对五角大楼的可视鉴定系统没有任何意义。所有的证件都是电子认证的，电子程序的安全性是世界级的。我还确信守卫身上的自动步枪是真的。

即使安检人员知道他们的职员戴着证件，我认为五角大楼的安全人员依然应当例行检查。我并不是对五角大楼说三道四，但是要提醒的是：即使最细心的政府机关雇用的工作人员也有粗心的时候。五角大楼的原则就是确保粗心的行为不会影响安全，企业的安全人员也应该把这一教训记在心里。职员的证件是一种不安全的鉴定机制。我们不能给社会工程师留任何空隙，应当建立一个安全的访问机制并要求大家执行，所有职员应理解并强制遵守这些政策。职员应当知道安全问题不是其他人而是自己的问题。

电子证件鉴定

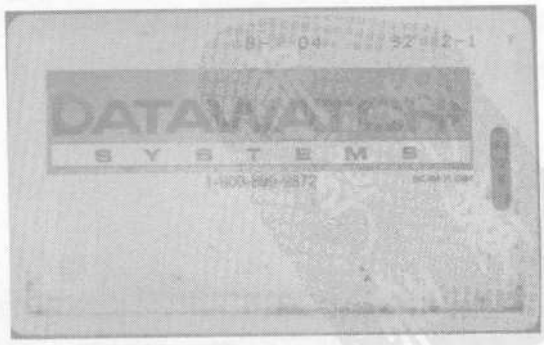
我想已经成功地确定可视证件鉴定系统是一种不可靠的安全机制。电子认证是一种更安全的鉴定方法，但是这些系统也有安全问题，非技术黑客对于攻击它们也非常感兴趣。平时看到一张接触式卡（proximity-type card）并不是很困难的

事，如下图所示。

高技术证件攻击

刷式卡、接触式卡或非接触卡应用的技术是不同的，但是它们可能被相近的方式攻击。它们都可被复制，这还多亏了 Jonathan Westhues 开发的装置（详情登录http://cq.cx/prox.pl），非接触卡隔着一些距离也能被复制，即使被放在口袋或钱包里。为了阻止此类攻击，可以考虑把访问卡与 PIN 认证方案结合起来、配置一个加密系统（挑战-响应系统）或读者访问清单，类似于 HiD 的 iClass。

这两个人具备很好的常识，拿掉了他们的证件。然而，他们的门禁卡仍然暴露在大家的视野里。虽然存在复制卡的可能性，但是对非技术黑客而言，选择性的攻击是可能的。一个敌人简单地看一下卡就能知道很多关于卡的东西，看下图中典型的 Datawatch 卡。



卡上面的通行数字号码可以通过 Datawatch 系统。要做的事情就是，告诉社会工程师那些通行号码，读出顶部一行的数字号码，可以获得大厦地址和号码，有时还会有房间号码。

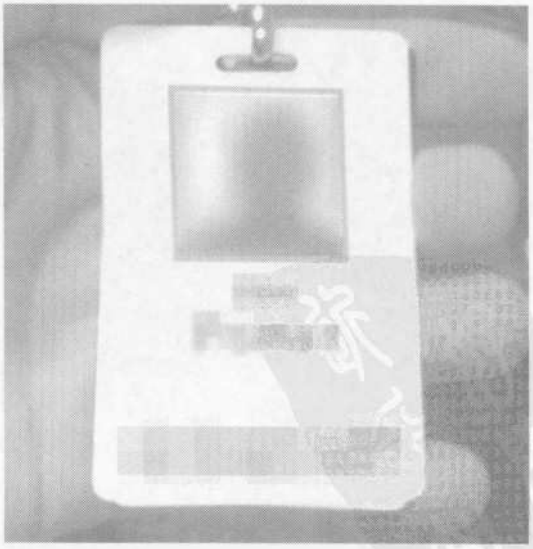
大部分人都不会把暴露了他们的工作地址的卡挂在前面，但是奇怪的是很多人却都戴着类似的可以暴露很多信息的电子卡。像这种访问卡在离开工作地方时应该拿掉。

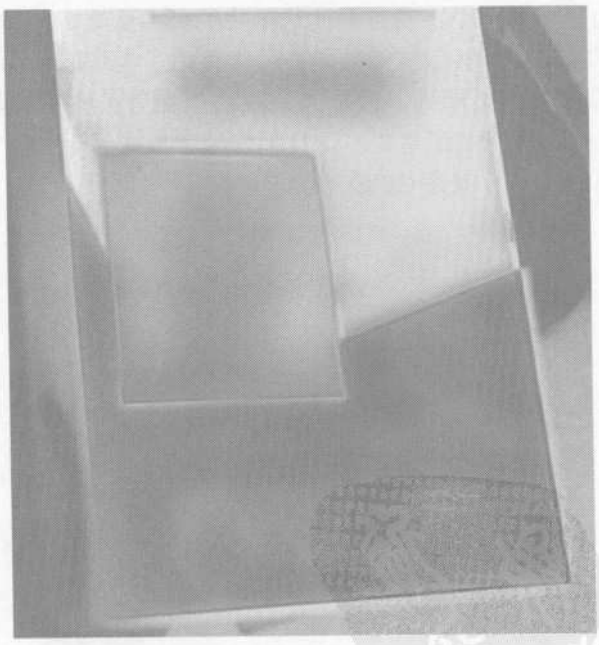
证件监视的真实世界

CP 告诉我一个故事，故事的内容是通过他的电话修理工证件进行的一次完美的社会工程攻击。CP 的风格让这故事更加可笑，因此我用他的话写下了这故事。

“一个电话公司的职员来我工作的地方修理 DSL2 线路，当他正工作时，我找了他的麻烦，含沙射影地说他也许不是来自电话公司的，我需要他的证件作为证明。他问我为什么要这个，我告诉他这是我的个人原则，他本可以不顺从的，然而他还是给了我证件，然后继续工作，同时我拍了 3 张证件的照片。当我用手机拍照时，他看上去有点紧张，但是之后我们坐在办公室里，我给了他雪碧和 Patron 酒，他没有拿酒而拿了雪碧，这样他好像才放松了下来。”

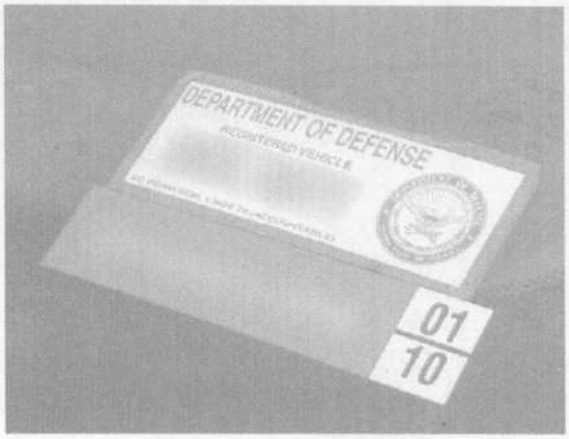
下面 3 张高清的照片就是 CP 成功的证明。





这次攻击简单而优雅。CP 把他的好奇心说成是个人的原则并给了那个技术员一个借口，使他看上去没有威胁（CP 的确是个好人）。通过一点饮料而让技术员麻痹大意，他很可能不会报告这个事件。假如 CP 是一个坏家伙，现在在你办公室的可能就是一个所谓的“非技术电话修理工”（伪装成电话修理工的攻击者）了。

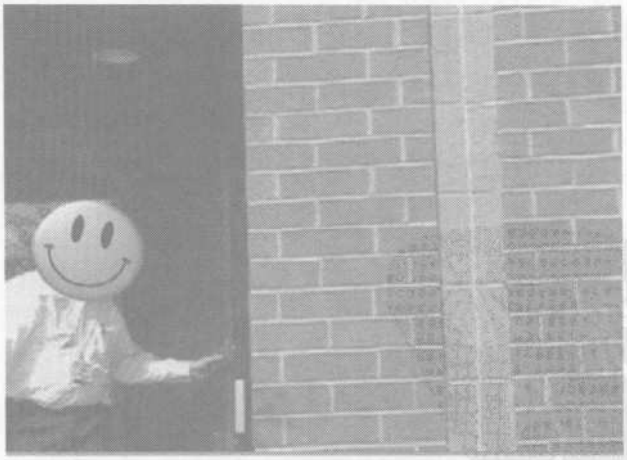
下面介绍的一个实际生活中的攻击是一个结合了两个技巧而进行的一次成功攻击。一天当我在开车兜风时，发现了一个戴着非常独特的蓝色政府证件的人在外面闲逛。我通过一个看似普通的办公停车场时，那个证件很让我吃惊。当我把车转过来想拍照时，已经找不到它的踪影了。我进入其中一个停车场，试着在周围找到那个政府办公楼。所有的楼房看上去都是一样的，并且大部分没有标记，这样更难找到它了。本来我想溜进一些大楼看一下，但由于这次不是一个收费进行的安全测试任务，搞不好会把我送到监狱里，我就打消了这个念头。为了寻找更多的证件，我还继续在停车场逛荡。然后我发现了一张熟悉的停车许可证。我走向那辆车，拍下了下面的照片。



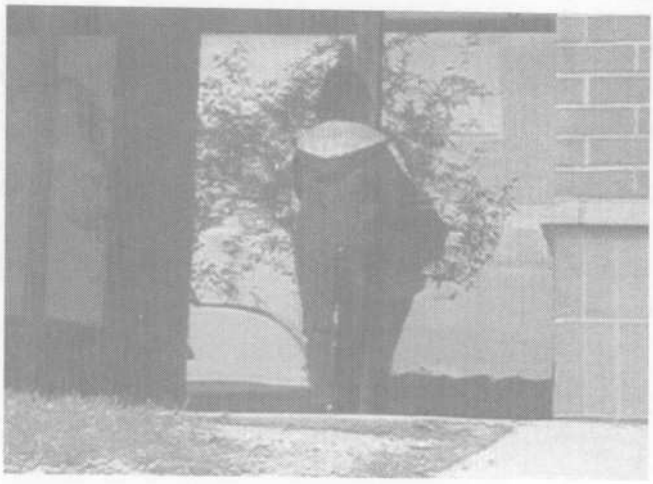
当我到这周围看看时，发现大楼周围的每辆车上都有一个国防部的停车许可证。我知道已经发现了政府大楼。我跳回车上，开始沿着这幢楼缓慢地转圈，仔细观察政府雇员。过了一会，我看到了一个人从大楼里出来了，如下图所示。看到了吗？

在那张图片中，蓝色证件十分清楚，我很快认出它是政府证件。当我驾车从窗口拍照时，照片上的家伙正好看着我这边，但是他好像没注意，他正忙着打电话。我决定停下我的车，沿着楼步行。当我从几个职员身边走过时，发现行走时很难去偷拍证件，因此放弃了偷拍，而是开始像一个普通人一样拍录像。随着举起相机，偷拍了下面一张录像的截图。

即使照片中的妇女注意到了我，她也没对我说任何东西。我也不认识她——我正忙着照相。接着我决定站在门口的一侧，用相机对着门口进行录像。我站在相机旁边，偶尔弯腰系鞋带（那天我并没有穿运动鞋）。这样让我看上去更不让人怀疑。我拍了很多类似下图的照片。



虽然有人看我站在路边感觉有点奇怪，但却没有一个人问我什么，因此在那多逗留了一会。下面的图片都是这样拍摄到的，下图是一个职员走进大楼。

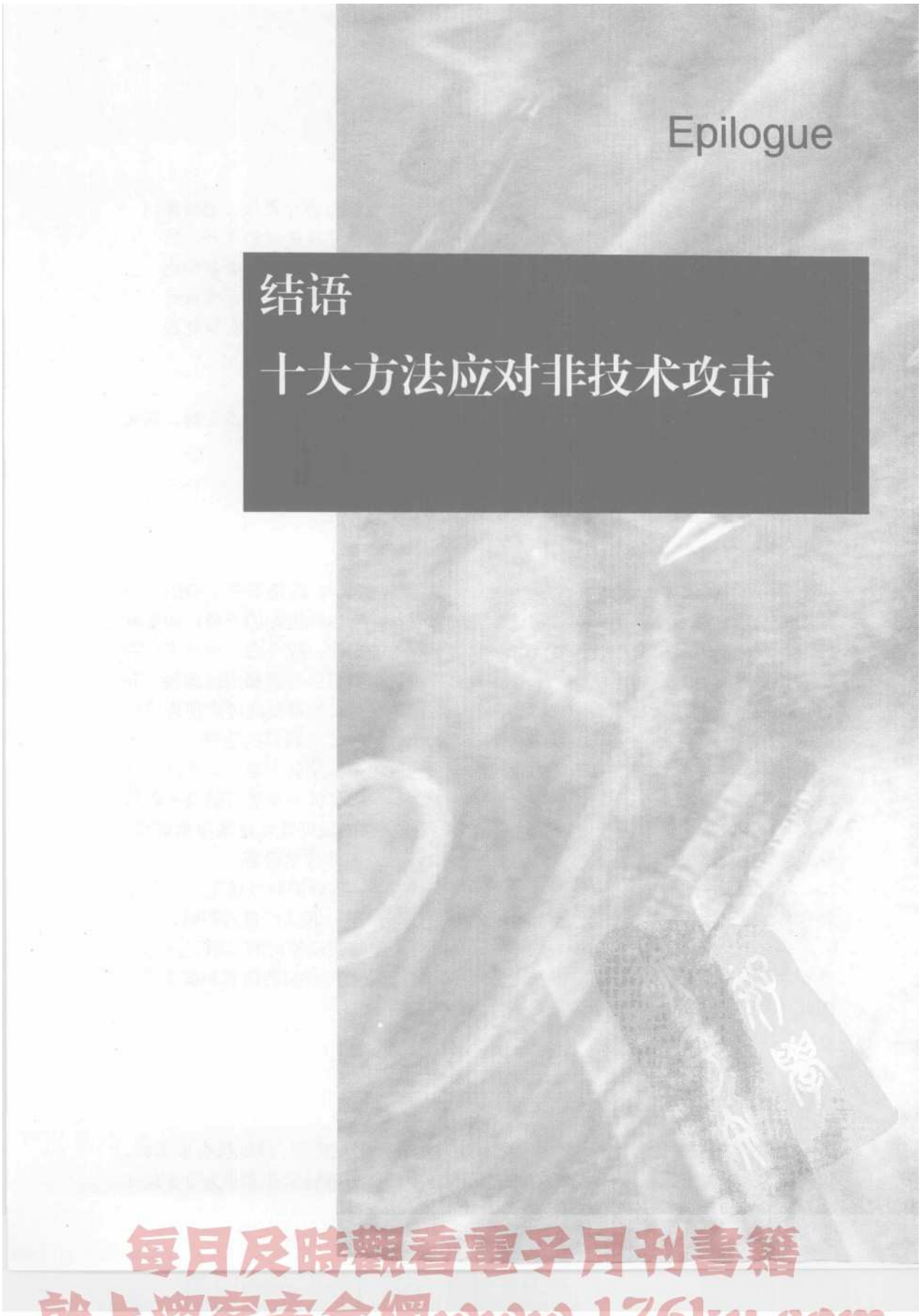


10s 后她通过了大门，此时门仅仅只关闭了一半。

这门要 15s 才能关闭，这是我看到的关闭最慢的门之一。这样的情况会使一个坏家伙有充足的时间在没有人注意的情况下溜进去。虽然我用这个政府大楼做例子，但是看过很多企业的大楼，它们比政府大楼更松懈、更不安全。这里要强调的是：尽管有高级安全系统，但是大部分还是要依靠人，而人通常是有惰性或缺乏相关知识的，或两者都有。非技术黑客知道这点，利用最有效的方法去攻击在安全上最脆弱的环节。你看到的本书的例子中，他们注意到我不仅监视他们，而且记录了他们及其环境。为什么他们不阻止或警告我？或许是他们中一些人并不关心这些。但是在大部分例子中，他们都没有反应，因为不知道该去做什么。如果你想要所在部门的人去挑战侵犯者或汇报异常事件，必须做好两件事：

- 对于可疑事件的汇报要实行奖励机制，这并不一定说是钱。在公司集会上的认可和表扬可以传达“警惕就是好的”这种信号，积极的人将得到奖赏。
- 确保想要的回应是大家都知道的且很容易做到。

坦白地说，如果看到我在你办公室或个人计算机前拍照，是否知道应该通知谁呢？同事？如果没人知道该怎么办，仅仅有“侵扰回应政策”是不够的。定期重复地宣传、复述它，下个月或许就有人知道了，一些非技术黑客正在等着你呢。



如果正在负责防范像我这样具有非技术攻击能力的坏家伙，必须要有以下清醒的认识。非技术黑客在公开的场合就能发现敏感的文档，除非你比他先发现。非技术黑客会注意柜子上的锁是否有作用，除非你比他先注意到。即使你没有听到哨声，但比赛已经开始了。你是否准备好和这个图谋不轨、目的明确的敌人斗智斗勇呢？如果没有，那么就赶在比赛结束前读读这本书，做好准备吧。

既然我们清楚坏家伙能够实现什么，回顾怎么做才能使他们走投无路。这是10种最好的应对非技术攻击的方法。

秘密进行

保守秘密 Gandalf 说，“保守秘密，就是保证安全”，这是非常正确的。不要在公众场合从事秘密的工作，别让自己成为目标。应当知道你的形象，如果有必要，保持低调。如果已经在公众的场合从事秘密的工作，应考虑一台膝上计算机的秘密过滤器。当然记住：一个有经验的背后偷窥者可以看到秘密过滤器，并能正确地猜测到你在从事的一些敏感东西。这样，一台过滤器反而可能使你或你的机器成为目标。不在公众的场所从事秘密的工作，这才是最好的选择。

行事低调 你或许因为工作的公司而自豪，但是炫耀团队不是个好想法。任何人都可能成为公众关注的目标或意料之外的目标。政府机关多年前就要求职员外出低调，但是这些人仍在使用明显的标志。我能提供的最好建议是做事低调点，花点时间考虑你的形象，三思而后行，至少应该先考虑非技术黑客。

不使用标签 如果你被迫在设备上贴公司的标签，出行的时候请把一张纸条粘在标签上。这至少可以让标签（可能涉及公司的信息）躲过好奇的眼睛。

别一起吃午餐 Jack Wiles 提醒在公众场所太容易谈论秘密的东西了，尤其当和同事一起共餐时。我们应该知道非技术黑客喜欢呆在企业的角落和餐桌边。因此，千万不要让公司的行话和秘密传入他们的耳朵里。

粉碎一切东西

最佳的方法就是粉碎一切东西。但是粉碎是一个主观的词。碎纸机有很多种，每种碎纸机提供的安全级别是不同的。一般的碎纸机切割的纸片大小为3/8英寸

（1 英寸=25.4mm），这就基本能满足需要了，重新组合的价值已经不高了。用微粒碎纸机处理文档非常好，但是非常昂贵。

一台微型碎纸机差不多要 200 美元，可以把纸、CD，甚至信用卡碎成 3/32×5/16 英寸大小的碎片，比一般的更安全。一般来说，碎纸机还是物有所值的，无论怎样处理都比把文档直接扔在垃圾里和停车场好。

在坏家伙知道之前知道你的垃圾里有什么东西也是个不错的想法。如果你负责公司的安全，每周都要到垃圾筒里看看都有什么东西将要被扔，并且要知道这些垃圾在被扔到室外的大垃圾桶时是什么样子的。如果想保护隐私，弄一台碎纸机，在家人扔垃圾之前和他们讨论哪些东西要碎掉。如果家人嫌麻烦，还得花时间好好说服他们。

买把好锁

我们倾向于选择一把好锁。我们已经看到许多锁可以用薄铝片打开。Deviant Ollam 说，我们能够通过选择好的锁来抵制这种攻击。下面就是他的建议：

- 选择一把只能用钥匙或密码关闭的锁。
- 选择一把保留钥匙的挂锁，当打开锁时，钥匙是挂在锁上的。
- 选择双球装置的锁。
- 选择类似手铐或脚镣的挂锁。

这是个非常好的建议，但我会不自禁地问道：“哪种锁是符合这些要求？”Deviant Ollam 和 Marc Tobias 给出直接的答案：

- EVVA MCS (www.evva.at/at/technology/mcs) 两位专家都认同的专业选择。
- Schlage Everest Primus (http://everestprimus.schlage.com) Deviant Ollam 和 Marc Tobias 都认为 Primus 非常好。Devian 说，“在大家发现安全问题之前，他们已经在做一把防凿防撞的锁了。”
- Abloy Protec (www.abloy.com.au) Deviant 说，“公司精心锤炼的设计让很多攻击无功而返。”
- Sargent & Greenleaf 8088 和 8077 系列锁(http://www.sargentandgreenleaf.com) 这种锁是用在国防部的文件柜上的。

Jack Wiles 也参与了评估，认为 ABUS Diskus (http://www.acelock.com)是一种“除了外形奇怪，其他都很好”的锁。

同样，必须谨记：无论锁多安全，都应该保持钥匙别让坏人看到。公开解锁组织的 Barry Wels 提醒我们，专业人员通过看一眼钥匙可能解读钥匙的信息，就有可能复制钥匙或者了解锁的构造。他在他的博客（www.toool.nl/blackbag）讲到一些监狱的警卫“用入狱者看不到的方式携带钥匙。”一个解决办法就是考虑来自www.key-port.com的、能根据客户需要修改的一种类似于“钥匙端口”的钥匙携带装置，可以从视觉上隐蔽钥匙，但当需要时可以很简单地取出来。

Jack Wiles 也提了一些合理的物理安全建议：

- 检查单位和家里所有的锁，排除任何故障。
- 不要让门一直开的。
- 回家前或怀疑有人闯入时，检查锁和钥匙。
- 考虑请一个专业人员去评估家或单位的物理安全。

放好证件

就像 Doris Troy 曾经唱的歌那样，“就一眼，带走了一切，是的，就一眼。”这就像一首非技术黑客的赞美诗。非技术黑客看一眼就能够记住一切、复制一切、渗透一切、破坏一切。放好证件，就这样简单。

检查监视装置

如果能绕过自己的安全摄像机和自动传感装置，坏人也可以（可能已经存在了）。检查所有的监视装置，考虑下面的建议。

- 质量好的摄像机不易受强光攻击的影响。
- 圆屋顶和薄膜也能够阻止闪光攻击，但记住任何光学处理都能够阻挡摄像机采光。
- 使用多个摄像机覆盖所有角落。
- 考虑房子装甲以及防止摄像机的传输缆线和电源被物理攻击。
- 隐藏的摄像机不会受到损害，尤其是和明显的摄像机混合使用时。

防止背后偷窥

注意你的角度 要知道偷窥者的角度，不要坐在会引来偷窥者的位置。当使

用机器时，要让位置是背对墙的，决不能没人看管机器就离开。不要佩戴公司的标志，把移动设备上的信息标志去掉，尤其是当公司的名字会引来对手时。商店里的技术支持人员能提供一些建议，帮助避免类似情况的发生，不妨听一听。

保守数据秘密　需要在公共场合输入密码时，需要注意什么呢？输入敏感数据时，在关键字和偷窥的眼睛间弄些障碍物。这或许需要移动身体，或利用空闲的手去遮挡。如果不想这样做，为什么还要密码呢？

Throw down!　我不建议用身体解决每个偷窥者。建议是，如果你认为成为了目标或突然对其他的东西感兴趣时（如想喝你的咖啡时），请关闭你的计算机（或关闭显示器）。大部分非技术黑客将知道他们已经失败了。如果他们的确离开，当他们离开时要不时盯着他们，在他们离开前试着看看他们及其交通工具。如果他们在离开时，想顺便看看你在忙什么，那就要考虑这样可能会带来什么危害，并有所行动。在关闭计算机后如果偷窥者还没有离开，无论如何也要注意了。如果他或她继续可疑的行为，那就要采取进一步的行动，通知管理人员、保安人员。可以采取一些行动，但如果动起手来，千万不要告诉法官那是我的主意。

防止尾随者

别放他们进去　如果你不认识的某个人企图在后面尾随，在黑客伸手时，拒绝他们进门，那样就可以把他们挡在外面。如果他们不是黑客，那就道个歉，请他们出去吃顿饭或许是个不错的选择。这样陌生人将害怕你，但是需要安全的人将会爱上你，这才是最重要的。

时刻保持警惕　千万别被事物的表面现象所蒙蔽。太多的人看到一个标志或一件制服就做很坏的假设，千万不要做这种人。如果第六感告诉某些地方不对，它很有可能就有问题。如果没有第六感，那就要随时准备一根木棒了。无论做什么事情，都不能让家庭和工作地方的安全依赖于可怜的假设。

禁止吸烟　我喜欢抽烟的入口，那是最喜欢的进入方法，即使那里有最安全的的设备。因此无论哪里都要禁止吸烟，破坏系统或许就仅仅是因为吸烟，要记住和你一起在外面的陌生人很可能就是我。

严格的制度　正如 Jack Wiles 说的，如果没有严格的制度要求所有职员去挑战不认识的人，“尾随”就是一个很难解决的问题。最少，如果他们怀疑一个没有被授权的人跟进来，职员应该知道什么时候以及怎么样通报安全部门。

清理汽车

标签不是朋友 非技术黑客通过查看汽车的标签就能得到很多东西。如果不是十分需要它们，就赶紧拿掉。最糟的就是加油卡、停车证和会员卡了。一些必需的标签不必一直贴在那。如果能够把它拿掉，那就把标签制成一个索引卡，不用的时候就放起来。

清理垃圾 记住一个八 P 格言：Printouts, paychecks, personal and private papers persuade peeping peoples（打印材料、薪水支票以及其他吸引偷窥者的私人物品）。现在来说，这句话并不是十分严密，但是我感觉它很有用。车里的垃圾不仅仅看上去不美观，而且能向别人提供一些信息。应该通过适当的信息精简来保护身份。

政府人员要行事谨慎 停车场汽车里的政府专用停车证就表明附近有政府部门。如果在一幢有许多这种停车证的大楼里工作，必须额外的警惕。必须警惕这栋楼或许就有尾随攻击、社会工程攻击、垃圾箱潜伏攻击或更坏的攻击手段的目标。

上网时留意背后

避免即时信息缺陷 我们能就使用即时信息（IM）程序而泄露秘密信息的事情写一整本书。注册一个新的 IM 账户目时，大部分服务内容都会产生很多私人数据，黑客或身份信息偷窃者可能会得到这些信息。决不要把个人信息透漏给一个陌生人。要确保客户程序的每个行为都是有效的，远程用户或许可能进行这些行为，如上传、下载等。如果关心隐私，配置很差的 IM 客户程序是很麻烦的。

关注点对点（P2P）软件 设想有一个黑客正在攻击私人信息，这的确很令人惊慌，但是要知道点对点攻击的不是特定的个体。点对点攻击是依靠特定的关键字找到感兴趣的信息。如果一个黑客在寻找你，他可能不会进入一个 P2P 客户端寻找你的信息，因为这要基于以下两个假设：你正在运行 P2P 客户端程序，并且已经共享了个人数据。这是两个相当疯狂的假设。因此如果真的运行了 P2P 软件，要确保在共享什么，并确保个人防火墙、防间谍软件都是最新的，并且配置正确。

搜索自己 即使没有过失，个人信息可能也会出现在网络上。如果它在网上，用 Google 就能找到它。如果 Google 能找到它，个人信息对黑客公开了。搜索自己决不是个坏办法，但是记住搜索整个信用卡号码或社会保险的号码数据就是个

坏办法，因为搜索本身变成了私人数据。相反，可以搜索姓名和地址，或姓名的一部分及一些敏感数字的一部分。

警惕社会工程攻击

那不是礼物 对于一个社会工程攻击者而言，他所关心的是得到一些东西。别人关注你的时候，你可能没有意识到，但无论什么时候一个陌生人从你那得到敏感信息都是有可能的。

经常保持意警惕 “电话里的每个未知声音都是潜在的社会工程攻击者。”Jack Wiles 说，“我不是偏执狂，只是小心。”

提前规划 如果你负责公司的安全，Jack 建议进行社会工程攻击教育，说明如何才能避免成为受害者。在能够使用的对策中，安全意识教育是最便宜和最有效的对策。他还建议模拟社会工程方法去完成任务，并且通过社会工程的攻击集中暴露与展示弱点，同时与职员们共同学习分享这些经验。